[doc. web n. 9703988]

Injunction order against the “Luigi Bocconi” Commercial University of Milan - September 16, 2021

Record of measures

n. 317 of 16 September 2021

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, which was attended by prof. Pasquale Stanzione, president, Professor Ginevra Cerrina Feroni, vice president, dr. Agostino Ghiglia and the lawyer Guido Scorza, members, and the cons. Fabio Mattei, general secretary;

GIVEN the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, concerning the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data and which repeals Directive 95/46 / CE, "General Data Protection Regulation" (hereinafter, "Regulation");

GIVEN the legislative decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national system to Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016, relating to the protection of individuals with regard to to the processing of personal data, as well as to the free circulation of such data and which repeals Directive 95/46 / EC (hereinafter the "Code");

GIVEN the Regulation n. 1/2019 concerning internal procedures with external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved by resolution no. 98 of 4 April 2019, published in the Official Gazette n. 106 of 8 May 2019 and in www.gpdp.it, doc. web n. 9107633 (hereinafter "Regulation of the Guarantor no. 1/2019");

Having seen the documentation in the deeds;

Given the observations made by the secretary general pursuant to art. 15 of the Guarantor Regulation n. 1/2000 on the organization and functioning of the office of the Guarantor for the protection of personal data, Doc. web n. 1098801;

Professor Ginevra Cerrina Feroni will be the speaker;

WHEREAS

1. Introduction.

With a complaint of the XX, as subsequently integrated on the XX, a student of the Commercial University "Luigi Bocconi" of Milan (hereinafter, the "University" or the "University") complained about possible violations of the data protection regulations

personal in relation to the use of a supervision system (proctoring) in the performance of the written exams of the students, in order to identify the students and / or to verify their correct behavior during the execution of the exam. . In particular, it was reported that the University would have requested the consent of the students to process "the particular categories of personal data (biometric data [...]), [in the absence of which the students] would not be able to take online exams" with this leading to “extreme prejudice […]”.

With the same complaint, it was highlighted that the data protection officer of the University, in response to the request for clarification from the interested party, clarified that, in the context of the epidemiological emergency from SARS-CoV-2, a alternative methods of conducting university exams at a distance, that the objective of ensuring the same guarantees provided for in-person exams could be achieved through the processing of particular categories of data, such as biometric data and that, after careful analysis, the University has identified the Respondus company as the best supplier to meet its needs, also taking into account the need to carry out about 60,000 / 70,000 written tests, having to ensure equal conditions for access to the tests for all students.

2. The preliminary activity.

With a note of the XX (prot. Of the Guarantor no. XX of the XX), in response to the request for information from the Guarantor, the University stated, in particular, that:

- "Bocconi University is an international, non-state university, legally recognized and authorized to issue higher education qualifications with legal value";
- "the recent orientation of the Council of State in the dispute between ANAC / non-state universities (for Bocconi CdS ruling no. 3041/2016; no. 3042/2016; no. 3040/2016) which qualifies the latter as subjects of private law , […] Believes that the only faculty recognized to free universities to issue qualifications with legal value is not in itself sufficient to determine their belonging to the category of public bodies. [...] "and, on this basis, the University would have identified the conditions of lawfulness of the treatment in question, taking into account its" qualification as a private entity ";
- in the context of the emergency situation caused by the SARS-CoV-2 epidemic, "in order to ensure the normal conduct of the examination sessions, given the impossibility of taking the tests as usual live and in presence, Bocconi has decided to equip itself with software ([…] “Respondus”) provided by the company Respondus Inc. ([…] the “Supplier”) - duly appointed as data processor pursuant to and for the purposes of art. 28 of the [Regulations] [...] which allowed the teacher to be able to verify the

authenticity of the written test given by the students, without it being altered, through substitutions of person and / or counterfeits, or other distorting interventions of the measure and evaluation of the 'personal learning';

- "the University has the duty to provide for all suitable measures to be able to consider fully valid the exams taken by its students [...], in order to guarantee the full legal value of the degree they have obtained";

- “Bocconi intended to adopt the proctoring system solely for the“ core ”courses, aimed at obtaining a qualification with legal value, as a method for guaranteeing impartiality, impartiality and equal treatment. For all the other training programs, however, the University preferred to take distance tests using different systems ";

- "the impossibility of carrying out the exam sessions according to the usual procedure, has led the University [...] to structure a process which, in compliance with the [Regulations] and the Privacy Code, only for written exams , was able to identify Students through the temporary use of their biometric data and, therefore, automatically processing the digital images depicting their faces for identification, authentication and verification purposes "in particular the" photo of the card "and “The photographic image taken by Respondus;

- with regard to the legal basis of the processing, the University stated that "for common data the legal basis has been identified in art. 6 lett. b) of the [Regulation]; for biometric data the legal basis was identified in art. 9 lett. a) of the [Regulation] ";

- despite "the provision of the Guarantor of 26 March 2020 and the d.p.c.m. of 27.4.2020 art. 1 letter n) ", the University," has chosen to consider for its students the option of the written exam online and remotely via proctoring system as the preferred route, for reasons of consistency with the didactic model adopted, based on consent. This is also in line with the private nature of the University ";

- the proctoring system was used for the first time in the summer session "which [...] began after the promulgation of the d.p.c.m. of 27.4.2020 and in particular, for all active study systems, in the period between 13.5.2020 and 21.7.2020 ";

- the University, "in order to guarantee the student's right to study, protecting their free self-determination, immediately put in place suitable organizational measures to allow the examiners, who may have decided not to grant consent to the processing of biometric data, to make use of alternative methods to be agreed with the Academic Services unit that manages the exam schedule ", without suffering" any harm or delay in the university career ";

- the information "pursuant to and for the purposes of art. 13 of the [Regulation] ";

- "The student's biometric data is not processed directly by the University, but only by the Provider who processes it temporarily for the duration of the exam session and then deleted without keeping it";

- “the processing does not matter an automated decision-making process. In fact, in the event that Respondus detects an anomalous event potentially capable of invalidating the exam, the software signals the anomaly to the teacher [...] who, in the exercise of its discretionary power of evaluation, will decide on the possible cancellation ";

- "the processing involves a transfer of data outside the EU by the Supplier" which declared to be "compliant with the EU-US Privacy Shield Framework";

- "the University, pursuant to Article 35 par. The deemed necessary to review the Nomination Agreement signed by Respondus ".

With a subsequent note of the XXth, the University integrated its feedback, providing, in particular, a copy of an additional document, dated XX, to the agreement on the processing of personal data stipulated with Respondus, Inc. pursuant to art. 28 of the Regulations, which encloses the standard contractual clauses, referred to in the European Commission Decision of 5 February 2010, stipulated between the University and Respondus, Inc ..

With a note dated XX (prot.no.XX, the Office, on the basis of the elements acquired, the verifications carried out and the facts that emerged as a result of the investigation, notified the University, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the measures referred to in Article 58, paragraph 2, of the Regulation, concerning the alleged violations:

of articles 5, par. 1, lett. a), 6 and 9 of the Regulations, as well as 2-sexies of the Code, for having processed the biometric data of students, as well as for having carried out an automated processing aimed at allowing the analysis of certain aspects of student behavior, therefore give rise to their "profiling", in the absence of an unsuitable legal basis;

of articles 5, par. 1, lett. a), and 13 of the Regulation), for not having provided the interested parties with complete information on the processing;

of art. 5, par. 1, lett. c) and e), and 25 of the Regulations, for having processed the personal data of students in a manner that does not comply with the principles of minimization, limitation of retention and protection of personal data from design and by default;

of articles 44 and 46 of the Regulation, for having transferred personal data to a third country, or the United States of America,

without having proven to have verified and ensured that the transfer in question was carried out in compliance with the conditions referred to in Chapter V of the Regulations;

of art. 35 of the Regulation, for not having carried out an adequate assessment of the impact on data protection with regard to the processing of personal data carried out through "Respondus".

With the same note, the University was invited to produce defensive writings or documents to the Guarantor or to ask to be heard by the Authority (Article 166, paragraphs 6 and 7, of the Code, as well as Article 18, paragraph 1, of the l. November 24, 1981, n. 689).

With a note from the XX (prot. No. XX), the University presented its defense brief, declaring, in particular, that:

the University has decided to "equip itself with proctoring systems", as well as other "universities which, during the pandemic period related to the emergency caused by Covid 19, made use of the system under discussion (or similar) [...,] in 'intent to be able to guarantee the rights of the [students] who have had the opportunity to continue - without any damage - the studies undertaken, despite the current emergency ";

"The particular emergency context [...] as well as the very short deadlines in which an effective and efficient solution had to be found [...] led Bocconi to believe that only a proctoring system could satisfy the real needs of its students - for the most part off-site and 19% of non-Italian nationality - and of the approximately 2,000 incoming exchange students who reach Bocconi every year from all over the world ";

"The University itself has never ceased to question the substitutability of the software implemented, perhaps even through other systems that were equally capable of guaranteeing the seriousness of the test. [...] In addition, the University has continued to have relations with Respondus to evaluate the functioning of the software implemented in an increasingly in-depth manner [, it being understood that] neither Bocconi nor Respondus, in fact, process the biometric data of students ";

"Respondus blocks the usability of the browser, effectively inhibiting the possibility that the student, during the period of the exam, can make use of aids present on his / her computer device - by this we mean both searches that can be carried out directly on the web and consultation of notes and / or handouts saved on the device itself in the form of files of different types - in order to take the test. In other words, Respondus Monitor does not keep track of the activity performed on the network by the student, of the applications in use, of the keys typed and of the mouse movements, but, more simply, it blocks the computer screen and prevents the student from all those interactions with the device that are not strictly related to the

performance of the exam ";

“It is […] completely unlikely that personal data or further information relating to aspects relating to the student's private life can be obtained through the system”;

"[...] in any case, the described system operates only and exclusively for the time corresponding to the duration of the exam [...]";

with regard to the alleged "profiling of the interested parties [...] the identification and evaluation of the test taken by the student and, therefore, the judgment and the correlated outcome of the exam, are completely left to the reference teacher, who is responsible for the evaluation. of the behavior of the student in practice: it follows that the system is merely limited to reporting, certainly not being able to be attributed a decision-making function. [...] The only aid provided by the software in question is the extract of some frames from the audiovisual recording, which could be indicators of anomalies during the test [...] ";

with regard to data retention times, "it is true that, in the abstract, the video recording of the exam could remain in the availability of the supplier's information systems for [...] one year on the AWS S3 bucket system plus four years , of long term storage, on the AWS Glacier system. However, the DPIA must be read in conjunction with all the provisions of the appointment as manager agreement [, on the basis of which] [...] [a] simple request of the University [...] the supplier [proceeds] both to cancel of the data, as to the notification of the cancellation. [...] Bocconi, in fact, requests that the aforementioned cancellation be carried out not after five years from the date of completion of the test, but once the exam session has formally closed and the evaluation procedure has been completed [...] of the tests supported by the students ". [...] [in any case,] "the video recording is not stored in clear text on the information systems of the University, so much so that the teacher does not have the ability to download said video, without the express authorization of the owner. In fact, the video is, until it is deleted, stored in a completely encrypted manner on the supplier's servers; only authorized persons within the University, for each individual test, hold the private key to make it readable. [...] With specific reference to the conservation of video recordings, Bocconi has deemed it appropriate to keep the same, in the manner detailed above, for a period corresponding to 12 months starting [from the date of communication of the test results to students], except on the single trial are not pending disciplinary proceedings or disputes before the competent judicial authorities. [...] Therefore, once the aforementioned terms have elapsed, the University destroys the only private key to access the encrypted data and requests, as described, the cancellation of the registrations also from the supplier. ";

in addition to the possibility of carrying out in presence in the event of the student's lack of consent, "the University has also concretely considered [...] to provide, for particular cases, such as students abroad, to take the oral exam online" ; moreover, “it is considered incorrect to state that giving the possibility to take the attendance exams would have exposed teachers and students to a higher risk to their health [, given the provisions of] [...] d.p.c.m. of 27.4.2020 art. 1 letter n) […] [, it being evident] […] that, with the appropriate precautions […] it was already possible to take the exams in person, obviously for those who did not want to give consent ";

the University "has a continuous dialogue with its student body which [...] cannot be considered on a par with a weak contractor, whose unequal position would legitimize stronger protection mechanisms. Certainly, the condition of presumed anxiety in which the student called to take the exam tests, or the metus towards the teacher, finds itself can in no way be considered as situations suitable to condition any consent given. [...] Especially when, as in the case [in this case], any refusal would not even have been expressed towards the reference professor, but only using the channels indicated by the University which provided for a specific request to Academic Services. And finally [...] in the event that the teacher puts in place "negative repercussions", the same will not be exempt from disciplinary responsibility for his own professional conduct [...] ";

the University has undertaken to "change the legal bases indicated in the information, without prejudice to the one identified for the processing of common data and modifying that for the processing of biometric data, identifying it in the pursuit of a public interest, pursuant to of the art. 9 letter g) of the GDPR and art. 2 ter and 2 sexies lett. bb of the Privacy Code ";

"However, with reference to the biometric data [...] [which] the short time available for the implementation of the process [...] led the University to rely on a statement by Respondus which subsequently proved not to correspond to the reality of the facts [...] following further investigations [...] Bocconi learned [that] the identification of the student took place and takes place retrospectively through a human operator, without using the biometric data for identification purposes [...] consequently, following a formal request from the University […], Respondus […] declared that the proctoring implemented does not involve any processing of particular categories of data […] ";

“[…] The system is not able to uniquely compare the student's face and the photograph of the document shown. In other words, in any case, for identification purposes, there is no creation of a biometric model of the individual student from which a biometric sample will be subsequently extracted to be kept for subsequent comparison operations (so-called match) ";" [...] also when checking the student's behavior, no biometric data is processed by the systems. The fact that the term "facial

recognition" is used does not necessarily imply that the systems set up for monitoring the student's behavior process the biometric data of the student ";

with regard to the dispute relating to the incompleteness of the information provided to students, the University points out that "the same disputed document refers to the complete information [...] through a specific hypertext link [...]";

"Bocconi acknowledges that the information could potentially lack transparency, since a specific retention period is not indicated";

"[...] taking into account the provision of art. 13 of the GDPR [...] the students [... have] received, on time, various instructions and clarifications well before the start of the treatment, with multilayer information [...] ";

kept the broad formula of lett. f) of art. 13 of the Regulations "the University in the disclosure identifies the article of the Regulation that allows the non-EU transfer of students' personal data, referring specifically to art. 46, and in any case leaves the interested party the possibility to "request more details from the Data Controller by requesting evidence of the specific guarantees adopted";

the University specified that it had stipulated "with Respondus, on the XXth date, a first agreement for the appointment of a manager, pursuant to art. 28 of the Regulation, with which, for what concerns the transfer of personal data outside the EU, it referred, pursuant to art. 46 of the Regulation, the Privacy Shield and, therefore, the then current Commission Implementing Decision (EU) 2016/1250. Following the ruling of the Court of Justice of July 16, 2020, it amended the appointment agreement and signed the standard contractual clauses as early as August 10, 2020 ";

"[...] the University [is] well aware of the measures taken by the supplier, considering that the same, although only referred to in appendix 2 of the signed standard contractual clauses, have been the subject of appropriate analytical assessments [...]. Even before the Schrems ruling, the University had put in place "the adoption of additional measures by the data controller in order to ensure compliance with this level of protection" (par. 133 of the Schrems ruling). The security measures […] have been attached to the DPIA itself […]. The entire impact assessment was carried out taking into consideration the Respondus Checklist document [...] from which it is evident that [...] personal data being processed are all encrypted with the Advance Encryption Standard 256 bit29 algorithm and the private key is held exclusively by Bocconi, so that it is impossible, even for the American government, to access them. In addition, Respondus Monitor among other things i) meets the security requirements of FERPA, GDPR, CCPA, Privacy Shield, SOC 2 and its engineers are also AWS Certified30; ii) all data is

encrypted from the beginning to the end of the process involving Respondus. This circumstance in itself determines compliance with the provisions of the European Court of Justice as well as the accountability of the University. The fact that reference is made to the measures, without attaching them to the undersigned, does not automatically imply that the assessment conducted by Bocconi, as data controller, is insufficient [...] The standard clause [...] itself provides that the exporter assumes the 'obligation to assess - by declaring and guaranteeing - that the importer provides sufficient technical and organizational safety measures, with no provision for how this obligation must be carried out. In other words, it is not legally required that the contract indicates the security measures in writing […] ad substantiam […] ";

"[...] the Recommendations 01/2020 of the European Committee for the protection of personal data - incapable of assuming the nature of a source of law, being soft regulation, and as such absolutely not binding - are subsequent to the violations currently contested. [...] In any case, [it should] be noted that, considering the types of personal data and the processing activities concretely implemented by Respondus, the measures set up are to be considered sufficient, and suitable, also and above all in light of the use systems of encryption of personal data and the actual inaccessibility of the same by third parties, including the responsible person and the US authority ";

"At the time when the choices for implementing the processes were made, it was considered that there were no other systems that could reasonably be able to guarantee, in digital form, the seriousness of the processes that had been built up to that moment in analog mode. It therefore appeared that the treatment according to the methods described was indispensable, because different digital systems would inevitably have been unsatisfactory for at least two reasons: a) on the one hand, because there are too many interested parties who make up the student body of the University (over 14,000 students) […]; on the other hand, the type of test - written exam - makes it impossible to achieve the prescribed purposes without the aid of proctoring systems [...]. The Court of Amsterdam also recently ruled on the proctoring system similar to the present one [, considering it compliant with data protection legislation] ";

"The legitimacy of this was also recently reiterated by the Spanish Guarantor according to which" The situation generated as a consequence of Covid-19 and the declaration of the state of alarm could have a special impact, in which the prevalence of facial recognition could be assessed with respect to to other measures [...] [, this option having to be limited] to those specific courses and subjects which, due to their importance, complexity or other circumstances of particular impact, do not make it advisable to use other options [...] or would make the adoption of other means such as video surveillance or excessively

expensive oral exams ";

as for the "reliability of the technology used [...] the University carried out a series of technical investigations on the security measures used by the company Respondus Inc. - market leader chosen by over a thousand universities - which are illustrated in the technical report [produced by the University] ".

At the hearing, required pursuant to art. 166, paragraph 6, of the Code and held on XX (minutes prot. No. XX of XX), the University, deviating with regard to certain profiles from the declarations made in previous communications, declared, in particular, that:

"Before the pandemic emergency, the tests were held in classrooms with a ratio of 1 to 3, or by summoning a student for every three places in the classroom, to ensure the effectiveness of the checks carried out by the physical" proctor ", who verified the identity of the student asking to show the card, as well as supervising the correctness of the test. [...] In this context, with only one teacher it was possible to follow the exam carried out by 50 people. The University therefore found itself, in the emergency state, in the condition of having to carry out the same tests but at a distance [...] The alternative of using a mere videoconferencing system supervised by a physical proctor would have probably required a proctor every five students to check. This alternative would not have been feasible, requiring the use of staff ten times higher than that available ";

"Only a dozen, of all the students who received the release form, wrote to the University and only a couple of these said they were against this method of conducting the test; however, these students did not follow up on the communications of the University, which had made itself available to find alternatives, and therefore there was no need to organize tests for these two students in different ways that did not foresee proctoring ";

"Starting from March 2020, the University began collecting documentation from the supplier and this documentation was found to have been drawn up in an exhaustive manner and in compliance with international standards. The supplier in this documentation and on its website mentioned the use of biometric technologies. However, in the context of the emergency, the University was unable to promptly verify what the alleged processing of biometric data consisted of. The University has therefore cautiously assumed that by biometric data we mean the type of data referred to in the definition provided in EU Regulation 2016/679. In fact, it later emerged that Respondus acquires the student's image and verifies that this face remains the same during the test, but does not relate the face to the person's identification. This identification is carried out by the teacher only later: the teacher, when he receives the report with the film of the test, compares a photograph taken by the

system at the beginning of the test with the photograph, present in the University archives, of the student who should have taken the same. Therefore, only in retrospect, it was possible to conclude that there was no use of a biometric data in accordance with EU Regulation 2016/679. It should be noted that, for the above, no extraction of the biometric sample relating to the student's face is carried out ";

“Respondus software has two components: Respondus lockdown browser and Respondus monitor. Lockdown browser behaves like a web browser because it displays the pages that are loaded and prohibits opening other pages or windows; it prevents, for example, the copy and paste operation. It also prevents the test from running if all other applications are not closed first. Therefore, when the exam begins, it is guaranteed that only browser lockdown is running and that the student only sees the exam page. At this point the test starts: during the test the student cannot do anything else that is not allowed by the system. Other functions of the PC are precluded and attempts to perform precluded activities are not tracked. In no case will any website be tracked. It is also possible to set the system in such a way as to allow you to visit certain sites or use certain applications that are useful for the sole purpose of taking the exam ";

"Respondus monitor is activated only after Lockdown browser has guaranteed the conditions necessary for the start of the test and detects and analyzes, for the purpose of defining the correctness index of the test, data such as, for example, the video, changes to the face subject to shooting or the absence of the same, the time for completing the test and answering each question, the keys typed on the keyboard, the movements of the mouse, the applications running (in order to possibly allow certain applications necessary for the execution of the test, it being understood that in the University's experience access to external sites has never been given; therefore, this function has not been used). As for the activity of the internet, the network traffic is measured and if this traffic has an anomalous amount of bytes, such as to presume a drop in the student's network bandwidth. Since there can be no other applications running, the system acquires only the data that is necessary to determine the correctness of the test. At the end of the test, the application closes and no more information is collected. After processing the collected data, the teacher receives a report showing the student's image for the purpose of identification and the indices of any anomalies, with details of the specific reason for the anomaly. The decision on the correctness of the exam is always the responsibility of the teacher. The video that is recorded cannot be downloaded; the teacher logs in with his own credentials and cannot see the videos of students who are not his own. The data is encrypted in transit. Furthermore, once the processing by the supplier is complete, the data is encrypted by the supplier, it being understood that the private encryption key is

available only to the University ".

With a subsequent note of the twentieth, the University sent a note sent by the company "Respondus" to the University, in which it is stated, in particular, that (text translated by the Guarantor from the original in English): no reports based on data relating to the timing of the test as well as data relating to the pressure of the keys on the keyboard, the movement of the mouse and the trackpad (unless they are used to switch between applications (for example, drag with three fingers) or to exit the system, this may lead to the generation of an alert); the number of interruptions and the duration of each interruption of the internet connection have an impact on the so-called Priority of the Review.

3. Outcome of the preliminary investigation.

3.1 conditions of lawfulness of personal data processing in the university environment.

As a preliminary point, it is noted that the freedom of teaching (see Articles 33 of the Constitution and 1 of Law No. 240 of 30 December 2010), even at university level, can be exercised by public or private subjects, regardless of the form legal status of the same (public bodies, foundations, corporations). The current legislation, in fact, does not expressly provide for the legal nature of non-state universities (or even "free universities" or "private universities"), limiting themselves to regulating single aspects of similarity or difference with respect to what is provided for state universities. Among the profiles of analogy with respect to the discipline of state (public) universities, there is, first of all, the pursuit of purposes of public interest (see Article 1, paragraph 1, of Law no.240 of 2010, referring to both state universities and to non-state universities). Furthermore, similarly to public universities, even private ones:

a) are subject to the same methods of establishment and suppression (arranged by decree of the Minister of Education, University and Research, within the three-year programming of the university system pursuant to art. decree of the President of the Republic January 27, 1998, n. 25);

b) are subject to the same provisions, with regard to the accreditation methods of university offices and courses (governed by decree of the Minister of Education, University and Research, in accordance with ANVUR's opinion, pursuant to art. 7 of the legislative decree 27 January 2012, n. 19);

c) have the power to attribute the same legal value to the qualifications issued (Article 167 of the Royal Decree of 31 August 1933, No. 1592; Article 4, paragraph 3, of the Ministerial Decree of 22 October 2004, No. 270 and Article 7 , paragraph 1, of the Presidential Decree of June 5, 2001, no. 328);

d) use the same methods of recruiting teaching and research staff, as most recently regulated by articles 18 and 24 of the l. 30 December 2010, n. 240 (see also art. 3 of Legislative Decree 165/2001);

e) recognize the same legal status to the teaching staff in service at state and non-state universities, pursuant to art. 6, paragraph 10, of the l. 30 December 2010, n. 240;

f) fall within the scope of the decree of the Presidential Decree January 27, 1998, n. 25, which provides that "in the event of the university being closed down, [...] teaching and research staff are guaranteed the maintenance of their posts, even in other universities";

g) are subject to the powers of direction and coordination by the Ministry of University and Research, pursuant to l. 9 May 1989, n. 168, powers which include, among other things, the legitimacy and merit control of the university statute and regulations (including the general one, the didactic one and the administration and accounting one), pursuant to art. 6, paragraphs 9 and 10, of the same l. n. 168 of 1989;

h) apply the same legislation on the right to study, as per Legislative Decree no. 68 of 2012.

With regard to these profiles, the Council of State has recently expressed itself, recognizing "the very significant general interest naturally covered by such activities and purposes", regardless of the nature and legal form of the person pursuing them (Consultative Section for Regulatory Acts, Section Meeting of 9 May 2019, no.1433/2019, which follows the Consultative Section for Regulatory Acts, Section Meeting of 31 January 2019, no. 370/2019).

Given that the regulatory framework on data protection provided for by the Regulation, which does not provide for a different regime applicable to public and private subjects, takes into account only the functional profile in the processing of data, it is believed that, given the prosecution of the same public interest, by public and private universities, the related processing of personal data is lawful if necessary "to fulfill a legal obligation to which the data controller is subject" or "for the execution of a task of interest public or connected to the exercise of public powers "(art. 6, par. 1, lett. c) and e), and, with regard to particular categories of data, art. 9, lett. g), of the Regulation).

For these reasons it is believed that, contrary to what was originally claimed by the University, the processing of student data for the purpose of issuing academic qualifications with legal value or those connected to the performance of activities subject to the supervision of the Ministry of University and Research cannot be founded on other legal bases such as consent and / or contract.

In this framework, the data controller is in any case required to comply with the principles of data protection (Article 5 of the Regulation) and, in the context of the necessary identification of the technical and organizational measures to guarantee and be able to demonstrate that the processing is carried out in accordance with the Regulation, also taking into account the specific risks deriving from the processing and in compliance with the principles of "data protection by design" and "protection by default" (Articles 24 and 25 of the Regulation), may have recourse to a person in charge for the performance of some processing activities to whom he / she gives specific instructions (cons. 81, articles 4, point 8), and 28 of the Regulation).

3.2 The processing of student data carried out through "Respondus" for the regularity of the remote exam tests. General consideration.

During the investigation it emerged that the University uses a remote supervision system for the written exams, called "Respondus" and provided by the company Respondus Inc. (established in the United States of America), structured in components "LockDown Browser" and "Respondus Monitor" to allow, in the context of the epidemiological emergency from SARS-CoV-2, the conduct of university exams at a distance with the aim of ensuring guarantees as much as possible equivalent to those provided for the exams in presence.

The Respondus Monitor software captures the video images and the student's screen identifying and flagging the moments in which unusual and / or suspicious behaviors are detected through video recording and snapshots taken at random intervals to track abnormal behaviors such as: non-gaze facing the monitor, face partially absent from the photo, face missing.

At the end of the test, the system processes the video, inserting warning signals regarding possible indices of incorrect behavior (so-called "flag") and assigning, among other things, a so-called "Review Priority", so that the teacher (supervisor user) can then evaluate whether an action not permitted during the test has actually been committed.

In this regard, it is noted, as a preliminary, that the need to verify the correct performance of the examination tests has assumed greater importance in the context of the epidemiological emergency from SARS-CoV-2, since, in order to ensure the continuity of teaching activities with methods compatible with public health needs, "remote" methods were favored for carrying out training activities and examinations.

With regard to the risks for data subjects deriving, from the point of view of data protection, from the use of systems for supervising the behavior of students during the remote exam tests, the Guarantor has recently highlighted that such systems "must not be unduly invasive and involve monitoring the student exceeding the actual needs ", since, although the necessary

compliance with the rules for carrying out the tests must also be guaranteed online, systems that involve" electronic surveillance without the necessary limits and guarantees "cannot be considered acceptable (see, Memo of the President of the Guarantor of 27 April 2021 at the 7th and 12th Senate Committees on the subject of "Impact of integrated digital teaching (DDI) on learning processes and on the psychophysical well-being of students", web doc. . 9581498, spec. Par. 2).

In this framework, therefore, universities, in carrying out their institutional tasks, which also involve checking the correct performance of the exams, even when they are carried out remotely, must comply with the principles of data protection, verifying, first of all place, the existence of the conditions of lawfulness with regard to the specific treatments deriving from the use of the supervisory systems and fulfilling, before the start of the treatment, the obligations of correctness and transparency towards the interested parties. This also in consideration of the particular invasiveness that the use of such technological solutions may, in some cases, entail (processing of particular categories of data; profiling; international data transfers).

3.3 The correctness and transparency of the processing: the information.

In compliance with the principle of "lawfulness, correctness and transparency", the data controller must take appropriate measures to provide the data subject, before starting the processing, with all the information required by the Regulation in a concise, transparent, intelligible and easily accessible form, with simple and clear language (articles 5, par. 1, letter a), 12 and 13 of the Regulation).

From an examination of the documents in place, it appears that the information on the processing of personal data provided to students (see Annex 5 to the note of the XX) does not contain all the information required by the Regulations to ensure correct and transparent processing. The document, which refers to the processing of biometric data and some other student data (name, surname and date of birth), only "by way of non-exhaustive example", does not mention the additional specific treatments put in place through the "Respondus" system, such as tracking the student's behavior during the test (face position; disconnections from the Internet network; attempts to use the mouse or trackpad to switch between applications or to exit the system; applications in use), the subsequent processing by profiling, the audio-video recording of the test. Nor is there any mention of the photograph taken by the system at the beginning of the test, the student, who is asked to show an identity document and to take a panoramic shot of the surrounding environment (see annex no. system technical report).

On this point, the University stated that the information originally provided to the students contained a reference "through a specific hypertext link" to the text of the "complete information on the processing of student data" (cf., defensive brief), however

not providing evidence in the course of the investigation.

From precise checks (see service report of the XX, in documents) it emerged, however, that the aforementioned hyperlink refers to web pages (https://www.unibocconi.it/privacy, which in turn bears a link to the page "Information for Students, Participants, Alumni and Donors") that actually carry generic information about the University treatments related to "school, academic or professional experience, the title of the thesis, the title of the final project, the duration of the studies and the results of the exams [, as well as the] documentation on the evaluation of your work, [...] ", without any specific reference to the treatments carried out through the" Respondus "system. Moreover, even the information updated on 7 October 2020, following discussions with the Office (see Annex 10 to the defense brief), does not however contain all the elements necessary to fully represent the processing.

Furthermore, the text of the information originally provided to the interested parties does not indicate the specific retention times of personal data, limiting itself to providing, in a generic way, that "the data will be kept for the period strictly necessary for the pursuit of the purposes indicated [... and] for a further period in the event that there is a need to manage any disputes or disputes "(see information of the XX sub annex 5 to the note of the XX). A similar generic wording is also contained in the version of the XX disclosure, although it contains some clarifications regarding the fact that "the [...] personal biometric data, which are not processed and stored by the university, will be deleted immediately by Respondus Inc at the end of each exam "(see annex 10 to the defense brief).

In this regard, it should be noted that "it is not sufficient for the data controller to state in a generic way that personal data will be kept as long as it is necessary for the legitimate purposes of the processing", having to set "different retention periods for the different categories of data personal data and / or purposes of the processing, including, where applicable, archiving periods "(" Guidelines on transparency pursuant to regulation 2016/679 "of 11 April 2018, WP260 rev.01, subsequently adopted by the European Committee on this point, the data controller has, in fact, declared that "as regards the retention period, in fact, Bocconi acknowledges that the information could potentially lack transparency, since a period is not indicated of specific conservation "(see defensive brief in deeds).

Again from the point of view of the correctness and transparency of the processing, the information does not mention that personal data are transferred to the United States of America, generally limiting itself to providing that "the [...] personal data will be processed by the Data Controller within and outside the territory of the European Union ", nor is the prerequisite for the

transfer specified, or - at the time - the Commission Implementing Decision (EU) 2016/1250, of 12 July 2016 on the adequacy of the protection offered by the shield EU-USA for privacy (Privacy Shield), as the students are not aware of the specific third country of destination of the data or of the particular guarantees adopted for such transfer, these guarantees being listed only by way of example. Moreover, even in the subsequent version of the XX disclosure (see Annex 10 to the defense brief), the specific third country of destination of the data (the United States of America) is not indicated. In this regard, the aforementioned Guidelines clarify that "the article of the regulation allowing the transfer and the corresponding mechanism [...] [, also providing] information on where and how to access or obtain the relevant document should be specified, for example . providing a link to the mechanism used. In accordance with the principle of fairness, the information provided on transfers to third countries should be as relevant as possible for data subjects. Generally, this means indicating the name of the third countries ".

It is also noted that, although the processing in question does not result in a fully automated decision-making process (see Article 22 of the Regulation), the information provided to the interested parties does not explicit the logic on which the functioning of the system is based. supervision (see Article 5, paragraph 1, letter a), of the Regulation). since the various system functions and the mechanisms that involve the generation of alarm / anomaly signals are not clarified, nor are the importance and consequences for the interested party disclosed in the event that certain behaviors are implemented during the course of the trial.

The need to ensure the correctness and transparency of the processing requires that the data subject be "informed of the existence of a profiling and its consequences" (cons. 60 of the Regulation) and that, regardless of the specific transparency obligations applicable to the decision-making process automated (articles 13, par. 2, letter f), and 14, par. 2, lett. g) of the Regulation), "the importance of informing data subjects of the consequences of the processing [...] and the general principle according to which this treatment should not surprise the data subject apply equally to profiling in general, not only to profiling described in Article 22 "(see," Guidelines on transparency pursuant to regulation 2016/679 "of 11 April 2018, WP260 rev.01; in general, on the need for data subjects to be duly informed about the" scheme execution of the algorithm and the elements of which it is composed ", see Civil Cassation Section I, Ord., May 25, 2021, no. 14381, which confirmed a previous provision of the Guarantor).

Nor can it be considered sufficient that "the representatives of the Students [...], even before the implementation of Respondus,

[had] been informed of the new process and its functionalities" (par. 3.3 of the defense brief), given that the information on processing of personal data must be "provided in writing or by other means, including, where appropriate, by electronic means" individually to each interested party. Having illustrated the functionality of the system only to the students' representatives is not, however, suitable for informing the interested parties individually with regard to all the processing operations carried out. Moreover, the information can be made orally only if requested by the interested party (see Article 12 of the Regulations). Also the "internal procedure for conducting online exams, widespread among students and the teaching staff" (par. 3.3 of the defense brief and annex 13 called "Guidelines for online written exams" which, moreover, in the version deeds, shows the date of XX), however not suitable for fulfilling the obligation to inform the interested parties pursuant to art. 13 of the Regulations, merely illustrates the technical and procedural aspects relating to the conduct of the remote examination tests, without illustrating the logic on which the “Respondus” supervision system is based.

In any case, in relation to the statement that the students would have "received, in time, various instructions and clarifications well before the start of the treatment, with multilayer information", it is noted that the approach of providing the interested parties with stratified information is useful for the purposes of compliance with the principle of transparency only if the first and second level information is presented to each other in a coherent and structured manner, allowing the interested parties to know the essential elements of the processing in the first first level information, and can then choose to deepen certain aspects in the detailed information (on this point, "Guidelines on transparency pursuant to regulation 2016/67" adopted on 11 April 2018, WP260 rev.01, par. 35, subsequently adopted by the European Data Protection Committee with "Endorsement 1/2018" of 25 May 2018: "the declarations / information on privacy are not mere pages nested in others that require several clicks to arrive at the desired information: the design and layout of the first layer of the privacy statement / information should be such as to offer the data subject a clear overview of the information available to him on the processing of personal data and the place and how he can find them between the different layers "). In the present case, however, the various information to students - which are in any case lacking with regard to the logic underlying the instrument used - was presented in a fragmentary and disorganized manner (and sometimes, as in the case of the indications given orally, which cannot be documented), without consistent references between the various documents (for example, the information on the processing of personal data does not mention at all the "Guidelines for written online exams" procedure).

For all the reasons described above, the treatment put in place by the University cannot be considered compliant with the

principle of lawfulness, transparency and correctness, since all the information required by the Regulation has not been provided (Article 5, paragraph 1, letter a), and 13 of the Regulation).

3.4 The absence of a legal basis for the processing of students' biometric data.

In response to the Guarantor's initial request for information, the University declared that it had structured "a process that [...] solely for the written exams, was able to identify students through the temporary use of their biometric data and, therefore, automatically processing the digital images depicting the face of the same for identification, authentication and verification purposes ", thereby confirming that the use of the system involved the processing of" biometric data "(art. 4, par. 1, n. 14), of the Regulation).

Subsequently, the University corrected its statements, stating, in the defense brief, as well as at the hearing, that following further investigations with the supplier, the system does not involve the processing of biometric data of the interested parties. Furthermore, in the technical report attached to the defensive brief (att. 16), it is stated that "the webcam video is analyzed using the Respondus technology, without biometric sample extraction" and that "various events reported largely depend on the technology of facial detection, which in no case involves the extraction of a biometric sample ".

First of all, it should be noted that, contrary to what the University claims, Respondus, Inc. stated that a biometric template is still generated, having specified that "the temporary biometric template does not correspond to any person identified in any internal database or external ”(see the note of the Respondus to the University of the XXth, sub annex 12 to the defense brief).

From what emerges from the documents, regarding the operation of the application, it is possible to state that the Respondus Monitor software carries out a specific technical treatment of a physical characteristic of the interested parties to confirm the presence and coincidence of the interested party for the entire duration of the test. Although the system does not involve the identification of the candidate - despite the preliminary actions of LockDown Browser it is expected that the student takes a photo of himself with the functions internal to LockDown Browser and exhibits an identification document (see technical report sub annex 16 to defensive memory) - and does not compare the image of the face with other images in its own database and in external databases, or does not carry out an identification (1 to many) or biometric verification (one to one), the system still carries out a treatment of biometric data which consists in the collection, processing and analysis of the video produced by the software through an artificial intelligence algorithm in order to produce the "flags".

For this reason, also taking into account what has already been stated by the Authority in similar cases, "in the case of facial

recognition, the prerequisite for the processing of images to be qualified as biometric treatment is that comparisons aimed at recognizing the individual (verification identity, in the case in question) are automated with the aid of specific software or hardware tools "(provision no. 345 of 26 July 2017, web doc. no. 6826368). For these reasons, given the definition of biometric data (art. 4, par. 1, n. 14, of the Regulation: "personal data obtained from a specific technical treatment relating to the physical, physiological or behavioral characteristics of a natural person who allow or confirm the unique identification, such as facial image or fingerprint data "), it is believed that the use made by Bocconi University using the Respondus software involves the processing of biometric data relating to the facial image of students. This circumstance is confirmed by the information on the processing of personal data, in the version of the XX (see Annex 10 to the defensive brief "the [...] biometric personal data, which are not processed and stored by the university, will be deleted immediately by Respondus Inc at the end of each exam ").

Having clarified this, the strengthening of the protections of biometric data provided for by the Regulation and the Code, as amended by Legislative Decree no. 101/2018 - due to their delicacy, deriving from the close and stable relationship with the individual and his identity - by including them in the categories of particular data and, like health and genetic data, among those assisted from a higher level of guarantees (Article 9, paragraphs 1, 2 and 4, of the Regulation; Article 2-septies of the Code), first of all concerned the legal conditions that make the processing of these categories of data lawful (see provision no.16 of 14 January 2021, web doc. no. 9542071). In this context, the processing of biometric data is generally prohibited, unless one of the conditions referred to in art. 9 of the Regulation "and in compliance with the guarantee measures set by the Guarantor".

In the present case, the University had identified in the student's consent the legal basis for the processing of biometric data processed through the "Respondus" system. However, as already specified in the previous par. 3.1, considering that the processing was carried out by the University for the purpose of issuing educational qualifications with legal value, contrary to what the University claims (see the opinion of the DPO and point 2.4., 3.1 and 5.1 of the impact assessment on data protection, in deeds), consent does not constitute the legal basis of the processing nor can it be considered a "manifestation of free will" (Article 4, par. 1, n. 11) of the Regulation), due to the imbalance of position of students with respect to the data controller (see recital 43 of the Regulations).

Although, in fact, only during the hearing, the University stated that "the Academic Services management, having consulted the

teacher, [...] found alternative solutions [to carrying out the test using the system in question] despite the constant state emergency (oral or written with videoconference and individual proctoring) ", with the press release of the XX, attached to the complaint, the students were warned that" in the absence of [...] consent, it will not be possible to take the exams online ", proposing as the only alternative the execution of the exam in person in a manner to be agreed with the teacher (see also par. 5 of the information of 24 April 2020:" any refusal to give consent for the processing of data biometric [...] will make it impossible to take the exam online and remotely. You will therefore be able to take the exam only live, in the real and not virtual presence of the reference teacher, at the University headquarters "). This, taking into account the emergency context deriving from the spread of the SARS-CoV-2 virus, can, on the one hand, expose teachers and students to a higher risk to health in the epidemiological context and, on the other hand, can generate fear in the student to suffer negative repercussions, even indirect ones, by teachers as a consequence of the refusal (see point 3.1 of the "Guidelines 5/2020 on consent pursuant to Regulation (EU) 2016/679" adopted by the European Data Protection Committee May 4, 2020).

Given the impossibility of recourse to consent, the processing of biometric data carried out by the University, attributable to the performance of public interest tasks, is permitted only to the extent that it is "necessary for reasons of significant public interest on the basis of 'Union or of the Member States which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to protect the fundamental rights and interests of the data subject "(Article 9, par. 2 , letter g), of the Regulation; art. 2-sexies, paragraph 2, lett. bb) of the Code defined the public interest as "relevant" for the processing carried out for the purposes of "education and training in the school, professional, higher or university setting"). In the margin of flexibility granted to the national legislator, art. 2-sexies of the Code specified the conditions required by art. 9, par. 1, lett. g), of the Regulation, delimiting the conditions of legitimacy of the processing, when they are necessary for reasons of significant public interest, the existence of a regulatory provision which must specify, in addition to the reason of significant public interest, among other things, the types of data, the operations that can be performed, the appropriate measures to protect the rights of the interested parties.

In this framework, therefore, in order for a specific treatment involving biometric data to be lawfully initiated, it is necessary that it finds its basis in a regulatory provision that has the characteristics required by the data protection regulations in terms of the quality of the source, necessary contents and compliance with the principle of proportionality (Article 6, paragraph 3, of the Regulation; on this point, albeit with regard to a different processing context, see provision no.16 of 14 January 2021, web doc.

no. 9542071). These elements, at present, have not been identified by any law or regulation of the sector or by the emergency provisions.

For these reasons, given that in the law in force there is no - nor has the University, indeed, identified - a legal provision that expressly authorizes the processing of biometric data for the purpose of verifying the regularity of the examination tests, the processing of the biometric data in question appears to have occurred in the absence of a suitable legal basis, in violation of Articles 5, 6 and 9 of the Regulations and art. 2-sexies, paragraph 1, of the Code.

3.5 Analysis of student behavior during the exam.

As it appears from the examination of the documentation in progress, the "Respondus" supervision system, in the component called "Respondus Monitor", is equipped with functions and mechanisms that involve the generation of alarm signals (so-called "flags") in order to detect anomalies of the student's behavior during the test to verify their correctness and consequent regularity. In particular, the document called "RespondusFeedback" (see annex to the note of the XX, cit.) Illustrates some examples of reports returned by the software on the basis of the analysis of the student's behavior during the test (eg position of the student with respect to web cam, disconnections from the Internet, applications in use, and mouse movements to switch from one application to another or to exit the system), allowing the teacher to view the frames with respect to which the system has highlighted an alleged anomaly (v. document "Additional Privacy Information - Respondus Monitor", published on the Respondus website, annex 11 to the defensive memory, in the version of the XX, where it is stated, in particular, that "Respondus Monitor continuously tracks the applications and processes that are running on the computer device during an examination session "; technical report sub. annex 16 to the defense brief; Respondus note of the XX, attached to the note of the University of the XX, with which the types of anomalous events detected by the system were specified).

The summary shown to the teacher shows the "Review Priority" index, "which indicates whether a student's examination session requires more attention from the teacher. The results are represented in the categories Low (LOW), Medium (MEDIUM) and High (HIGH) with a bar graph from green to red indicating the level of risk "; the “Review Priority” value comes from three data sources: the student's webcam video; the computer device and network used for the test; the student's interaction with the test [...] "taking into account various anomaly indices such as, for example, video interruptions, the automatic restart of a webcam session, attempts to change the application; Furthermore, various anomalies "largely depend on the facial detection technology" which is able to signal the absence of the candidate or the replacement of a person (see

technical report cited).

In light of the set of elements that emerged during the investigation and while taking into account the University's corrections and clarifications, it is believed that the functions of the "Respondus Monitor" component, which determine a partially automated processing for the analysis of the behavior of interested parties, according to the subsequent evaluation of the teacher, give rise to a "profiling" of the students (Article 4, par. 1, n. 4, of the Regulations), understood as the operation of automated processing of personal data "for evaluate personal aspects relating to a natural person "and, in particular, as in the case in question, to analyze aspects concerning the behavior or reliability of the data subject (Article 4, No. 4, of the Regulations).

Especially in the context of the exercise of public interest tasks, as in the case in question, it is necessary to take into account the specific risks deriving from profiling, which, generating new and additional information from that provided by the data subject or acquired elsewhere, can sometimes lead to detrimental consequences. for the interested party, such as, in general, the exclusion from benefits, the lack of access to goods and services or, as in this case, the cancellation of an exam, in violation of the principle of non-discrimination. Therefore, the processing in question, in order to be lawful, in addition to having to be clearly represented to the interested parties, must be, in this context, necessary for the performance of a task of public interest and must therefore be provided for by a law or regulation. regulation (art. 6, par. 1, lett. e), and par. 3, and cons. 72 of the Regulation, art. 2-ter of the Code) which, however, does not exist in the present case.

For these reasons, it is believed that the described treatments consisting in the analysis of students 'behavior during the examination test the processing of students' personal data was carried out in violation of Articles 5, par. 1, lett. a) and 6 of the Regulations.

3.6 Data protection by design and by default, minimization and limitation of retention.

Apart from the observation of the absence of the legal basis of the processing, from the documentation in the file it is clear that the "Respondus" supervision system is not limited to inhibiting specific functions of the devices used by the students during the course of the exam (through the 'use of the so-called “LockDown Browser” function only). Through the "Respondus Monitor" extension, the system keeps track of the student's behavior during the test (disconnections from the Internet; attempts to use the mouse or trackpad to switch from one application to another or to exit the system; applications in use; position of the student's face), generating a plurality of information and personal data relating to the student and his / her conduct, the

processing of which is not strictly necessary to ensure the proper conduct and validity of the test. Moreover, some of this information, as in the case of the applications in use on the student's terminal, are potentially suitable for revealing aspects relating to his or her private life.

Also in consideration of the risk incumbent on the rights and freedoms of the data subjects, the data controller, also making use of the support of the data protection officer, must "from the design stage" and "by default" (Article 25 of the Regulation) adopt adequate technical and organizational measures to implement the principles of data protection (Article 5 of the Regulation), such as the principles of minimization and limitation of conservation referred to in Articles. 5, par. 1, lett. c) and e) of the Regulation) and integrating in the processing the necessary guarantees to meet the requirements of the Regulation and protect the rights and freedoms of the data subjects (see "Guidelines 4/2019 on article 25 Data protection by design and by default ", adopted on 20 October 2020 by the European Data Protection Board, spec. points 42, 44 and 49). This also when the data controller uses products or services made by third parties, giving the necessary instructions to the service provider if necessary and making sure that, for example, the functions that have no legal basis or are not compatible with the purposes are deactivated. of the processing (see, in particular, with regard to the processing of user and employee data through a service booking system at the counter, provision 17 December 2020, no. 282, web doc. no. 9525337, but already provision 7 March 2019, n.81, web doc. N.9121890).

Furthermore, considering that personal data must be "stored in a form that allows the identification of data subjects for a period of time not exceeding the achievement of the purposes for which they are processed" (Article 5, paragraph 1, letter e) , of the Regulations), it is noted that, with regard to the retention times of the audio-video recordings of the exams (i.e. five years from the date of the exam - see par. of the XX -, then reformulated by the University in twelve months following the administrative dispute - see defensive brief), the owner has not provided the specific reasons on the basis of which it would be necessary to keep the data for such an extended period of time. On this point, it should be noted, in any case, that this retention period is not proportionate with respect to the purpose of ensuring the regularity of the examination tests. Nor can this long period of time be justified for the further purpose linked to the use of the same data in the event of any disputes by the interested parties, considering the terms established by law to challenge the outcome of the test (complaint to the examining commission or appeal to the Regional Administrative Court).

As traditionally stated by the Guarantor, the processing of data carried out for the purpose of protecting one's rights, including

in court, as stated in the information provided to students, must, in fact, refer to ongoing disputes or pre-litigation situations, and not to abstract ones. and indeterminate hypotheses of possible defense or protection of rights (this general principle was, lastly, reaffirmed by the Guarantor, albeit in a different context, in the "Provision containing the provisions relating to the processing of particular categories of data, pursuant to art . 21, paragraph 1 of legislative decree 10 August 2018, no. 101 ", annex 1, paragraph 1.3, letter d), doc. web n. 9124510; v. also prov. 8 March 2018, n. 139, doc. web n. 8163433, par. 4.1).

Also at the European level, although in the matter of international transfers of personal data, the European Data Protection Board stated that "the use of the derogation [from the general transfer ban] to justify the transfer of personal data on the basis of of the mere possibility of any legal proceedings or formal procedures in the future "(" Guidelines 2/2018 on the exemptions referred to in Article 49 of Regulation 2016/679 "adopted on 25 May 2018), thus confirming that the processing of data for protection of one's rights in court cannot depend on the possibility of a merely possible dispute.

As for the fact that, as declared by the University, the impact assessment on the protection of personal data, where the five-year retention period is indicated, must be read together with the provisions of the data processing agreement stipulated with the supplier, pursuant to which the data controller may ask the supplier to delete the data at any time, and that, on the basis of these forecasts, "Bocconi, in fact, requests that the described deletion be carried out after five years from the date of completion of the test, but once the exam session has formally closed and the [...] procedure for assessing the tests taken by students has been perfected "(see defense brief), it is noted that, in compliance with the principle responsibility, the data retention times must be established ex ante by the data controller in a certain and documentable manner (see art.5, par. 2, 24 and 25 of the Regulation). Otherwise, the data controller could not inform the data subjects about the data retention times before starting the processing (see articles 13, paragraph 2, letter a) and 14, par. 2, lett. a) of the Regulation) and, in the context of the impact assessment on data protection, as in the present case, could not carry out a complete "assessment of the needs and proportionality of the processing in relation to the purposes" (Article 35, par . 7, lett. B) of the Regulation), also with regard to the "limitation of conservation (article 5, paragraph 1, letter e))" ("Guidelines on impact assessment on data protection and determination of the possibility that the processing "may present a high risk" for the purposes of Regulation (EU) 2016/679 "of the Article 29 Working Group, adopted on 4 October 2017, WP 248 rev.01, adopted by the European Committee for the protection of data with "Endorsement 1/2018" of 25 May 2018).

With regard to the University's assertion that "the video recording is not stored in clear text on the information systems of the

University [...] [, being the] video [...], until its cancellation, kept in a fully encrypted manner on the servers of the supplier "(see defense statement), it is noted that, even if the data in question reside on the IT systems of the supplier, which therefore processes the data on behalf and in the interest of the owner (see cons. 81, art. 4, point 8), and 28 of the Regulation), it is however on the latter that the "general responsibility" (cons. 74 of the Regulation) related to the processing weighs (see articles 5, paragraph 2, and 24 of the Regulation), also with regard to the certain definition of data retention times (see Article 5, paragraph 2, of the Regulation, pursuant to which "the data controller is responsible for compliance with paragraph 1", or the applicable principles to the processing of personal data, including the principle of limit conservation action).

For the reasons represented, the processing of students' personal data is carried out in a manner that does not comply with the principles of data protection from the design stage and by default, minimization and limitation of storage, in violation of Articles 5, par. 1, lett. c) and e) and 25 of the Regulations.

3.7 International transfers of personal data

As emerged from the investigation, the supervision system used by the University is provided by Respondus, Inc., a company established in the United States of America, which processes personal data as data processor, on the basis of a processing agreement. of personal data ("Appointment of an External Data Processor under Regulation (EU) 2016/679"), stipulated between the parties on date XX pursuant to art. 28 of the Regulation.

In this regard, in general, it is noted that transfers of personal data to countries not belonging to the European Economic Area are allowed provided that the adequacy of the third country has been recognized by a decision of the European Commission (see articles 44 and 45 of the Regulation). In the absence of such a decision, the transfer is permitted provided that the data controller provides adequate guarantees that provide for enforceable rights and effective remedies for the data subjects (Article 46 of the Regulation). In this regard, the standard data protection clauses adopted by the European Commission (Article 46, paragraph 2, letter c), of the Regulation, may constitute adequate guarantees.

In the absence of any other prerequisite, it is possible to transfer personal data on the basis of some exceptions that occur in certain specific cases (Article 49 of the Regulation), which must be strictly interpreted and which can only be applied in the case of occasional and non-occasional transfers. repetitive (see the "Guidelines 2/2018 on the exemptions referred to in Article 49 of Regulation 2016/679", adopted on 25 May 2018 by the European Data Protection Board).

With reference to the transfer of personal data to the United States of America, the Court of Justice of the European Union,

with its judgment of 16 July 2020 (Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18), has declared invalid the decision relating to the so-called Privacy Shield (Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection offered by the EU-US Privacy Shield), in consideration of the fact that the internal law of United States of America (in particular Article 702 of the Foreign Intelligence Surveillance Act - FISA and Executive Order 12333) - allowing public authorities, within the framework of certain national security programs, to access personal data without adequate restrictions object of transfer for the purposes of national security - does not guarantee a level of protection substantially equivalent to that recognized by European law and does not grant interested parties rights that can be enforced in court against the US authorities.

The Court also examined the validity of the Commission Decision of 5 February 2010 relating to the standard contractual clauses for the transfer of personal data to data controllers established in third countries, and considered their validity, on the assumption that such clauses aim solely at providing contractual guarantees that apply uniformly in all third countries, regardless of the level of protection guaranteed in each of them. However, since these clauses, taking into account their nature, do not provide guarantees that go beyond a contractual obligation to respect the level of protection required by European Union law, "they may require, depending on the situation existing in the one or the other third country, the adoption of additional measures by the data controller in order to ensure compliance with this level of protection "(paragraph 133 of the judgment). Therefore, the data controller has the obligation to verify, case by case, and possibly in collaboration with the recipient of the transfer, whether the law of the third country of destination guarantees adequate protection, in the light of European Union law, of the data. personal data that are transferred, providing, if necessary, additional guarantees with respect to those offered by the standard clauses. If it is not possible to adopt these additional measures, it is necessary to “suspend or put an end to the transfer of personal data to the third country concerned” (paragraph 135 of the judgment). This hypothesis occurs, in particular, "in the event that the law of that third country imposes on the recipient of a transfer of personal data from the Union obligations in contrast with said clauses and, therefore, capable of calling into question the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to such data "(ibidem).

Art. 8.2 of the data protection agreement stipulated between the University and Respondus, Inc. provides that "the Data Controller authorizes the Data Processor to process or transfer data outside the European Union, provided that the Data Processor guarantees that there are mechanisms that can ensure an adequate level of protection and that the interested

parties have enforceable rights and effective means of appeal ".

The transfer of personal data, relating to students and staff of the University, to Respondus, Inc. was carried out on the assumption that, as stated in the University note of the XXth, Respondus, Inc. "declares and guarantees, by means of the own privacy policy published at the following electronic address https://web.respondus.com/gdpr-privacy-shield/, to adhere to the Privacy Shield ", in accordance with the European Commission Implementing Decision (EU) 2016/1250, of 12 July 2016 on the adequacy of the protection offered by the EU-US Privacy Shield.

As a consequence of the aforementioned judgment of the Court of Justice of the European Union of 16 July 2020 (Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18), which invalidated the aforementioned Implementing Decision (EU) 2016/1250, the University entered into with Respondus, Inc., on 18 August 2020, an additional act to the data protection agreement, called "Amendment to Appointment of an External Data Processor under Regulation (EU) 2016 / 679 ". This act reports, in annex, the standard data protection clauses referred to in the Commission Decision of 5 February 2010 relating to the standard contractual clauses for the transfer of personal data to data processors established in third countries, bearing the date of 20 August 2020.

Appendix no. 2 to the standard contractual clauses (Appendix 2) provides that "the data importer must implement administrative, physical and technical measures to protect the security, confidentiality and integrity of the Personal Data uploaded for the use of the products granted licensed "and that" the details relating to these measures are available on the Respondus Monitor Hecvat module, which can be consulted on request at the following address: https://web.respondus.com/hecvat/ "(" details regarding these safeguards are available on the Respondus Monitor HECVAT form, which is available upon request via URL: https://web.respondus.com/hecvat ").

In this regard, it should be noted that the description of the technical and organizational security measures, carried out in these ways, is however not suitable to meet the provisions of art. 4, par. 1, lett. c) the standard contractual clauses, pursuant to which, "the exporter declares and guarantees [...] that the importer will provide sufficient guarantees as regards the technical and organizational security measures indicated in Appendix 2", specifying, in the following lett. d), that "in light of the legislation on data protection, the security measures are designed to guarantee the protection of personal data [...]" (similarly, Article 5, letter c), of the standard clauses provides that "The importer declares and guarantees the following: [...] c) that he has applied the technical and organizational security measures indicated in Appendix 2 before proceeding with the processing of the

personal data transferred"). This in particular taking into account that these technical and organizational measures are not attached to the signed contract, being made available, only upon request through an online request form, and there being no certainty as to which measures are actually adopted by the importer, with with regard to the specific transfer, as they may vary over time (however, without the exporter necessarily being aware of it), and the obligation contractually assumed by the importer in terms of safety is not clearly identified.

Moreover, the defense thesis of the University cannot be accepted, according to which the University was in any case "well aware of the measures taken by the supplier" and that these measures were "attached to the DPIA itself [or to the impact assessment on the protection of data] ", there is a" only formal relatio [...] because the determination of the measures refers to an element that, although external to the agreement, is known to both parties ". In fact, it must be considered that Articles 4, par. 1, lett. c) and 5, lett. c) of the standard clauses, referred to above, expressly provide that the security measures must be "indicated in appendix 2" and that in the same appendix 2 it is specified that it "constitutes an integral part of the contractual clauses and must be completed and signed by the parties ", Contemplating a specific section, called" Description of the technical and organizational security measures implemented by the importer in accordance with clause 4, letter d), and clause 5, letter c) (or the document / legislative act annex) " .

In the documentation provided, however, the technical and organizational measures have not been specifically described, it being only indicated that they can be obtained by the owner upon request. It should also be considered that, pursuant to art. 3, par. 1, of the standard contractual clauses attached to the decision of the European Commission 2010/87 / EU, "the interested party may assert, against the exporter, [...] clause 4, letters b) to i), clause 5, letters from a) to e) […] as third party beneficiary ", including, therefore, Articles art. 4, par. 1, lett. c) and 5, lett. c) mentioned above.

It is therefore evident that, since the parties have not indicated with certainty, in Appendix 2 to the standard clauses, the specific security measures to be adopted, the interested parties, as third party beneficiaries, cannot enforce the commitments undertaken contractually regarding security in the against the exporter, in violation of the provisions of art. 3, par. 1, mentioned above, being irrelevant for this purpose that the security measures to be adopted were in any case known to the parties stipulating the standard clauses.

From another point of view, with reference to what was considered by the Court of Justice in the aforementioned judgment of 16 July 2020, it is not clear from the documents in the file that the exporter has carried out an assessment of the effective

capacity of the measures adopted to guarantee compliance with the obligations undertaken. by the importer with the signing of the aforementioned clauses, in light of the legislation of the third country to which the data must be transferred.

In particular, considering that personal data are transferred to the United States of America, a third country whose internal law, as established in the aforementioned judgment of the Court of Justice, does not guarantee a level of protection substantially equivalent to that recognized by the European law and does not grant the interested parties rights that can be enforced, in court against the US authorities, the University, in the context of the stipulation of the standard contractual clauses, should have expressly assessed and envisaged, if necessary, "the adoption of additional measures by the data controller in order to ensure compliance with this level of protection "(paragraph 133 of the sentence), an assessment of which there is no evidence in the contractual documentation stipulated with Respondus, Inc. and provided to the Guarantor.

In this regard, it is noted that, as clarified in the "Recommendations 01/2020 on the measures that integrate the transfer tools to ensure compliance with the level of protection of personal data of the European Union", adopted by the European Committee for the protection of personal data on 10 November 2020, in the event that the domestic law of the country in which the importer is established (in this case the United States of America) imposes obligations on the latter that are in contrast with those provided for by him charged by the standard contractual clauses (and it is not possible to put in place additional measures capable of ensuring compliance with these obligations), the owner is required to suspend the transfer of the personal data in question to the third country in question and / or resolve the clauses standard contracts stipulated with the importer, as required by art. 5, lett. a) and b), of the contractual clauses themselves.

The same considerations also apply to the transfer of the personal data in question to the sub-processor, indicated in Appendix no. 2 to the standard contractual clauses, namely Amazon Web Services Inc., also established in the United States of America.

In fact, the documentation stated by the University in its memoirs is not reflected in the fact that "the measures taken are to be considered sufficient, and suitable, also and above all in the light of the use of encryption systems for personal data and the actual inaccessibility of the same by third parties, including the person in charge and the US authorities ". As specified by the University during the hearing, in fact, personal data "are encrypted in transit" and then, "once the processing by the supplier is complete", they "are encrypted by the supplier, it being understood that the private encryption key it is available only to the University ". It follows that the encryption of the data with the University key takes place only after the processing of the same

by the supplier, who, in order to be able to examine the videos relating to the exams and determine the risk index (also by means of the processing of biometric data of the interested parties), must therefore necessarily access the data in clear text, as they are encrypted only at the end of this process. This is also confirmed in the technical report produced by the University attached to the defense brief ("the system underlying the operation of Respondus Monitor takes about 8/12 hours to prepare the video for the teacher to view, because the algorithm that processes the video It is very accurate. Once the videos relating to the exam taken by the students have been processed, the "Class Results" function will be enabled in the Respondus Monitor dashboard, where teachers will be able to access information on the exam sessions ").

Nor can the mere pseudonymisation of the data transferred abroad be considered sufficient (see the attached technical report: "the video files, relating to each student's test, are conveyed by the APIs connected to the LMS to the SaaS system that Respondus holds on AWS "and that" session identifiers containing pseudonymised data and that do not contain personal data are therefore generated "), since, even assuming that the pseudonymisation could be effectively carried out in the case in question, taking into account the specific data processed (eg registration of examination tests), it is, in any case, to be considered "a processing of personal data" (Article 4, No. 5, of the Regulations) aimed at ensuring the security of processing (see art. 32, paragraph 1, letter a) of the Code, where “pseudonymisation” is mentioned among the possible technical measures adequate to guarantee a level of security adequate to the risk). Pseudonymization is not the same as data anonymization.

In consideration of the above, the University has therefore transferred personal data to a third country, or the United States of America, without having proved that it has verified and ensured that the transfer in question was carried out in compliance with the conditions. referred to in Chapter V of the Regulations, in violation of articles 44 and 46 of the Regulation. This circumstance assumes particular importance given that, among the data subject to international transfer, there are also data relating to particular categories, such as biometric data.

3.8 The data protection impact assessment

In implementation of the principle of accountability (see Article 5, paragraph 2, and 24 of the Regulation), it is up to the owner to assess whether the treatments that are intended to carry out may present a high risk for the rights and freedoms of individuals - in reason for the technologies used and considering the nature, object, context and purposes pursued - which requires a prior assessment of the impact on the protection of personal data (see cons. 90 and art. 35 of the Regulation).

From the examination of the documents in place, it emerged that the impact assessment on data protection, although carried out by the University, was not carried out in a completely adequate manner, limiting itself to illustrating the characteristics of the supervisory system used, representing it as compliant with legislative framework on data protection, without however a precise assessment "of the necessity and proportionality of the treatments in relation to the purpose" and "of the risks for the rights and freedoms of the data subjects" (art. 35, par. 7, lett. b) and c)), also in terms of possible influence or indirect pressure on students, reporting extremely concise judgments of adequacy, without suitable motivation (see, in particular, paragraphs 3 and 4 of the impact assessment in the proceedings) , having therefore not been identified, in relation to certain profiles, appropriate measures "to address the risks" and to mitigate them (Article 35, paragraph 7, letter d) of the Regulation). In particular, in the impact assessment on data protection prepared by the University:

in par. 3.3, relating to compliance with the principle of minimization, it is generally acknowledged that "the University believes that the data processed are adequate, relevant and limited to what is necessary with respect to the purposes pursued, not collecting data beyond those necessary for carrying out the test written exam. conformity assessment: positive ", not reporting a timely assessment of the adequacy, relevance and proportionality of each category of data processed by the supervision system, with particular regard to the data relating to the analysis of the student's behavior during the test, and, therefore, without providing a suitable justification for the positive judgment;

in par. 3.4, relating to compliance with the principle of accuracy, it is generally stated that “the personal data - common and biometric - of the Student must be exact, otherwise the indicated purposes could not be pursued. conformity assessment: positive ", not detailing an adequate assessment of the actual reliability of the supervision tool, with regard to both facial recognition functions (for example to verify that malfunctions do not occur due to skin color or somatic traits linked to the ethnic origin of the interested parties), and to the mechanisms by which the risk indices are defined, having therefore not been assessed the possible repercussions for the interested parties in the event of errors or false positives / negatives. Moreover, in par. 7 of the impact assessment, the risk related to discrimination was assessed as "unlikely", with potential "average" damage, as "no discrimination could be determined", without, however, a prior assessment of the reliability of the algorithms used by the supervisory system. Moreover, inconvenient measures are indicated for the mitigation of the risk of discrimination ("the system is built in such a way as not to allow the conservation of biometric data. Protection from intrusion through firewalls, absence of exposure on the network and encryption on transit traffic") .

With regard to "reliability in terms of personal data protection", the University stated, in its defense brief, that "the University has carried out a series of technical investigations regarding the security measures used by the company Respondus Inc . - market leader chosen by over a thousand universities - which are illustrated in the technical report [attached to the memoirs] "; this technical report, which is undated, was, in any case, provided by the University after the date of notification of the violation, thereby finding implicit confirmation that the impact assessment on data protection had not adequately addressed this aspect. Although the technical report states that "even if a student's examination session receives a" High Review Priority ", it does not mean that an illegal action has taken place. Many data contribute to a priority classification and some, such as an interruption of the Internet service or low quality video, are not necessarily indicators of prohibited behavior. Due to the high traffic on the network, especially in this historical period, it is likely that students may suffer this type of interruption ", thereby confirming that human intervention is required to make decisions towards the interested party, it does not appear, however, that the University has identified the criteria on the basis of which the teachers, reviewing the video of the exam, can evaluate and decide in practice whether the interruption or degradation of the video is due to a technical problem or to a student misconduct. Nor does it appear that specific instructions have been provided on this point to teachers, in order to ensure equal treatment of students, as well as the accuracy and homogeneity of the assessments of the reported events, with possible repercussions on the validity of the test.

In relation to compliance with the conservation limitation principle, the University limited itself to reporting the retention times of the data declared by the supplier in the "in the form in the Privacy Shield Framework" and in the "Checklist Respondus", without any timely assessment, from the perspective of the owner, regarding the appropriateness of these retention times with respect to the purposes of the treatment pursued;

in par. 4, relating to the “necessity and proportionality of the processing”, it is generally reported that “the processing is necessary for the pursuit of the purposes set out. The data collected are, in fact, adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ", without explaining the assessments made by the owner regarding the reasons why it was necessary to adopt a supervisory tool. remote exams equipped with facial recognition functions and able to profile the behavior of students during the test, as well as the reasons why it was not possible to use alternative supervision tools, but less invasive for their rights and freedoms ;

in par. 7, with regard to potential "physical or mental damage", the University's analysis focused solely on the possible

psychological damage deriving from the "disclosure of exam records", evaluating the risk as "unlikely" and the potential damage as " medium ", without, however, considering that, regardless of any disclosure of the recordings, the impact on the emotional and psychological sphere of the data subjects may also derive from the specific functions of the supervision system, such as, in this case, facial recognition and the profiling of behavior, with possible repercussions on the accuracy of the anomalies detected by the algorithm and therefore, indirectly, also on the overall outcome of the test.

4. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the data controller during the investigation □ the truthfulness of which one may be called to respond pursuant to art. 168 of the Code □, although worthy of consideration, do not allow to overcome the findings notified by the Office with the act of initiation of the procedure and are insufficient to allow the dismissal of this proceeding, since none of the cases provided for by the 'art. 11 of the Guarantor Regulation n. 1/2019.

Therefore, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by the University is noted, for having, in violation of Articles 5, par. 1, lett. a), c) and e), 6, 9, 13, 25, 35, 44 and 46 of the Regulation, as well as 2-sexies of the Code.

The violation of the aforementioned provisions entails, pursuant to art. 2-decies of the Code and "except as provided for in Article 160-bis", the unusability of the personal data processed.

The violation of the aforementioned provisions also makes the administrative sanction provided for by art. 83, par. 5, of the Regulation, pursuant to art. 58, par. 2, lett. i), and 83, par. 3, of the same Regulation and art. 166, paragraph 2, of the Code.

5. Corrective measures (art. 58, par. 2, letter d), of the Regulation).

Art. 58, par. 2, lett. f), of the Regulation provides that the Guarantor has the corrective powers to "impose a temporary or definitive limitation to processing, including the prohibition of processing".

Taking note of what emerged during the investigation phase and taking into account the fact that the "Respondus" system is not discontinued by the University, it is necessary, pursuant to art. 58, par. 2, lett. f) of the Regulations, order the limitation of processing, prohibiting the University from any further processing operations, with regard to the biometric data of students and the data on the basis of which the profiling of the interested parties is carried out through the "Respondus" system, and prohibiting the transfer of the personal data of the interested parties to the United States of America, in the absence of adequate guarantees for the same.

Pursuant to art. 58, par. 1, lett. a), of the Regulations and 157 of the Code, the University must also communicate to this Authority, providing an adequately documented feedback, within thirty days from the notification of this provision, the initiatives undertaken in order to implement the above ordered pursuant to the aforementioned art. 58, par. 2, lett. f), as well as any measures put in place to ensure compliance of the processing with the legislation on the protection of personal data.

6. Adoption of the injunction order for the application of the pecuniary administrative sanction and ancillary sanctions (articles 58, par. 2, lett. I and 83 of the Regulation; art. 166, paragraph 7, of the Code).

The Guarantor, pursuant to art. 58, par. 2, lett. i) and 83 of the Regulations as well as art. 166 of the Code, has the power to "inflict an administrative pecuniary sanction pursuant to Article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, depending on the circumstances of each single case "and, in this context," the College [of the Guarantor] adopts the injunction order, with which it also disposes with regard to the application of the ancillary administrative sanction of its publication, in whole or in excerpt, on the website of the Guarantor pursuant to Article 166, paragraph 7, of the Code "(Article 16, paragraph 1, of the Guarantor Regulation no. 1/2019).

In this regard, taking into account art. 83, par. 3, of the Regulation, in the present case - also considering the reference contained in art. 166, paragraph 2, of the Code - the violation of the aforementioned provisions is subject to the application of the same administrative fine provided for by art. 83, par. 5, of the Regulation.

The aforementioned administrative fine imposed, depending on the circumstances of each individual case, must be determined in the amount taking into account the elements provided for by art. 83, par. 2, of the Regulation

In relation to the aforementioned elements, it was considered that the processing also concerned data belonging to particular categories, with respect to which the regulatory framework for the protection of personal data provides for a higher level of protection, and concerned a large number of interested, in consideration of the fact that the University has, according to what has been declared, "over 14,000 students"

On the other hand, it was considered that the University, in facing unprecedented problems deriving from the emergency context determined by the Sar-Cov-2 pandemic, had to make choices and adopt technical and organizational measures quickly in order to ensure the continuity of teaching activities and the conduct of the exam sessions. Furthermore, with regard to the violation of articles 44 and 46 of the Regulation, it was considered that the judgment of 16 July 2020 of the European Court of Justice (Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, Case C-311/18) was issued

when the treatments in question were already that the consequences of the legal principles formalized therein may, in some cases, be complex to implement, as well as, more generally, that the legal framework on international transfers is still evolving (see the "Recommendations 01 / 2020 relating to the measures that integrate the transfer tools in order to ensure compliance with the EU level of protection of personal data "of the European Data Protection Board of 10 November 2020, which at the time it was placed in be the conduct had not been definitively adopted; see also the recent European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 relating to the contractual clauses current type for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, effective from 27 June 2021). Finally, it was favorably acknowledged that, despite the contradictory statements made on certain profiles, the University has substantially proved to be cooperative and willing to accept the Authority's findings.

Furthermore, there are no previous violations committed by the data controller or previous provisions pursuant to art. 58 of the Regulation.

Due to the aforementioned elements, assessed as a whole, it is believed to determine the amount of the financial penalty in the amount of € 200,000.00 (two hundred thousand) for the violation of Articles 5, par. 1, lett. a), c) and e), 6, 9, 13, 25, 35, 44 and 46 of the Regulation, as well as 2-sexies of the Code, as a withheld administrative fine, pursuant to art. 83, paragraph 1, of the Regulation, effective, proportionate and dissuasive.

Taking into account the particular delicacy of the data processed, it is also believed that the ancillary sanction of the publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Guarantor Regulation n. 1/2019.

Finally, it is noted that the conditions set out in art. 17 of Regulation no. 1/2019.

WHEREAS, THE GUARANTOR

notes the unlawfulness of the processing carried out by the "Luigi Bocconi" University of Milan for violation of Articles 5, par. 1, lett. a), c) and e), 6, 9, 13, 25, 35, 44 and 46 of the Regulation, as well as 2-sexies of the Code, in the terms set out in the motivation, and declares, pursuant to art. 2-decies of the Code, the unusability of data processed in violation of the relevant regulations on the processing of personal data, except as provided for by art. 160-bis of the Code;

ORDER

at the "Luigi Bocconi" Commercial University of Milan, in the person of the pro-tempore legal representative, with registered

office in Via Sarfatti, 25 - 20136 Milan (MI), Tax Code 80024610158, pursuant to articles 58, par. 2, lett. i), and 83, par. 5, of the Regulations, to pay the sum of Euro 200,000.00 (two hundred thousand) as a pecuniary administrative sanction for the violations indicated in the motivation; it is represented that the offender, pursuant to art. 166, paragraph 8, of the Code, has the right to settle the dispute by paying, within thirty days, an amount equal to half of the sanction imposed;

INJUNCES

to the aforementioned University:

a) to pay the sum of € 200,000.00 (two hundred thousand) in the event of failure to settle the dispute pursuant to art. 166, paragraph 8, of the Code, according to the methods indicated in the annex, within thirty days of notification of this provision, under penalty of the adoption of the consequent executive acts pursuant to art. 27 of the l. n. 689/1981;

b) pursuant to art. 58, par. 2, lett. f) of the Regulations, the limitation of processing, prohibiting the University from any further processing operation with regard to the biometric data of students and the data on the basis of which the profiling of the interested parties is carried out through the "Respondus" system, as well as prohibiting the transfer of personal data of data subjects in the United States of America in the absence of adequate guarantees for the same;

c) pursuant to art. 58, par. 1, lett. a), of the Regulation and 157 of the Code, to communicate to this Authority, providing an adequately documented feedback, within thirty days from the notification of this provision, the initiatives undertaken in order to implement the aforementioned order pursuant to the aforementioned art. 58, par. 2, lett. f), as well as any measures put in place to ensure compliance of the processing with the legislation on the protection of personal data.

HAS

pursuant to art. 166, paragraph 7, of the Code, the publication of this provision on the website of the Guarantor, considering that the conditions set out in art. 17 of the Guarantor Regulation n. 1/2019;

the annotation of this provision in the internal register of the Authority, provided for by art. 57, par. 1, lett. u), of the Regulations, violations and measures adopted in compliance with art. 58, par. 2, of the Regulation.

Pursuant to art. 78 of the Regulation, 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision, it is possible to appeal before the ordinary judicial authority, under penalty of inadmissibility, within thirty days from the date of communication of the provision itself or within sixty days if the applicant resides abroad.

Rome, September 16, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Geneva Cerrina Feroni

THE SECRETARY GENERAL

Mattei