- SEE ALSO NEWSLETTER OF 2 AUGUST 2021

[doc. web n. 9685922]

Injunction order against Aeroporto Guglielmo Marconi di Bologna S.p.a. - June 10, 2021

Record of measures

n. 235 of 10 June 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 the "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 4/4/2019, published in the Official Gazette n. 106 of 8/5/2019 and in www.gpdp.it, doc. web n. 9107633 (hereinafter "Regulation of the Guarantor no. 1/2019");

GIVEN the documentation in the deeds;

HAVING REGARD to 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;

Rapporteur Prof. Ginevra Cerrina Feroni;

WHEREAS

1. Introduction.

As part of a cycle of inspection activities, concerning the main functions of some of the applications for the acquisition and management of reports of offenses most widely used by public and private employers within the framework of the regulations on reporting illegal conduct (so-called whistleblowing), specific investigations were carried out against the companies Aeroporto Guglielmo Marconi di Bologna S.p.a. (hereinafter the "Company" or "AdB"; see the minutes of the operations carried out in the twentieth century) and aiComply S.r.l. (hereinafter "Supplier", see minutes of the operations carried out in the twentieth century), which provides and manages on behalf of the Company the application called "WB Confidential". This also in light of the provisions, with regard to the initiative inspection activity carried out by the Guarantor's Office, with resolutions of 12 September 2019, doc. web n. 9147297, of 6 February 2020, doc. web n. 9269607, and of 1 October 2020, doc. web n. 9468750.

2. The preliminary activity.

At the outcome of the investigation, given the particular complexity of the technological profiles that emerged during the investigation (see technical report of the XX, prot. No. XX), it emerged that:

- the data controller - publicly held stock company for about 45% of the share capital and listed on regulated markets, the sole operator of Bologna airport, as public service concessionaire until 28 December 2044 by virtue of an agreement with the National Civil Aviation Authority (ENAC) - adopted an organization, management and control model pursuant to Legislative Decree no. 231/2001 which, with the entry into force of law n. 179/2017, was integrated and updated with a specific "whistleblowing policy", using the "WB Confidential" application;

- the application is made available by the Supplier in SaaS (Software as a Service) mode, for the acquisition and management of reports of illegal conduct. To this end, the relationship with the Supplier, as data processor, has been regulated pursuant to art. 28 of the Regulations (see minutes of the XXth, spec. Annex 10 - designation deed);

- the Company makes available a disclosure pursuant to the Regulations "to reporting subjects in the process of sending a report using the WB Confidential application, accessible at the web address http://whistleblowing.bologna-airport.it/". The same information "is made available in the information section of the same application, together with the Whistleblowing Policy and the User Manual for the use of the application" (see minutes of XX, p. 4) also for the benefit of interested parties who may be mentioned within the reports received by the Company;

- "the sending of reports [is allowed] both by employees and by other stakeholders. Reports can be submitted in anonymous or

nominative form with the aid of the WB Confidential application or in nominative form through the use of dedicated e-mail boxes, as required by the Whistleblowing Policy. In both cases, the only person authorized to process the data of the reports, by accessing the application or the aforementioned e-mail boxes, is [... the] head of the Internal Audit function [... who], when accessing the application, does not have the visibility of the identifying data of the reporting party which are logically separated from the content of the report. Only in certain cases, established in the Whistleblowing Policy, [... the manager] can learn about them upon express request to the company aiComply S.r.l. " (see minutes of the 20th, p. 5);

- "following the sending of a nominative report, the application issues the reporting party with authentication credentials (username and password), which the same can use to access the application and follow the progress of the report as well as carry out an integration , also at the request of the Head of the Internal Audit function. In the case of anonymous reporting, it is necessary to access the application with dedicated authentication credentials, listed in the User Manual ". As for nominative notifications, "additional authentication credentials (username and password) are issued to the reporting party" (see minutes of the XXth, p. 4);

- moreover, "upon receipt of a report via the application [... the manager] receives a notification email on their inbox. On the basis of the case in question, [...] evaluates the involvement of the Ethics and Anti-Corruption Committee or the Supervisory Body, taking care to remove, if necessary, the elements from which it is possible, even indirectly, to trace the identity of the reporting. In certain circumstances, the identity of the reported person may also be omitted. If the conditions are met, the report is also forwarded to the General Manager and / or to the Managers of other company functions, to the Human Resources Manager for disciplinary profiles and / or to the Judicial Authority in the case of criminally relevant facts "and in any case "the identity of the whistleblower can be disclosed to the aforementioned subjects only in the cases" provided for by the sector law (see minutes of XX, p. 5);

- the Company "has a single account for access to the application, assigned to the [... manager], who is assigned the privileges of managing the reports received"; moreover, as verified during the investigations, "in the presence of a nominative report, the manager is not authorized to view the identification data of the reporting party" and that "each report is assigned an identification code (called" ID Ticket ") with format of the type "SA-WB00000042" or "SN-WB00000052", where the letters "SA" or "SN" indicate respectively the anonymous or nominative character of the report while the digits represent the progressive number assigned to the report ";

- during the checks, the presence of two anonymous reports was found on the application, one of which was archived (see minutes of the 20th, p. 5);

- the processing is "registered in the register kept pursuant to art. 30 of the Regulation ";

- the Company stated that it did not consider it necessary to carry out an impact assessment on data protection pursuant to art. 35 of the Regulation, "also taking into account the small number of data processed and the interested parties involved in the processing in question" (see minutes of the XX, p. 2);

- it was verified that the application, exposed on the Internet, does not use a secure network protocol (such as the https protocol) for the transport of data and the Company has on the point represented that it has initiated evaluations about "the opportunity to this measure is in place to guarantee the confidentiality and integrity of the data transmitted on the public network "(see minutes of XX p. 3);

- with regard to the methods of surfing the Internet by employees who are connected to the company network, with particular regard to navigation on the "WB Confidential" application, the Company stated that "access to the public network takes place via firewall systems new generation, which allow you to configure specific Internet browsing rules, also due to the role of the different functions and tasks performed by individual employees [... and] that these firewall systems store the browsing operations carried out in special log files, whose storage term is set at 90 days, specifying that no specific precautions have been envisaged in order not to register navigation operations on the WB Confidential application "(see minutes of XX, p. 3).

During the inspections carried out at the Supplier (see minutes of the XX, pp. 2 et seq.) It emerged that:

- the same offers a "specialized maintenance activity, both at the system level and at the application level, in relation to the application [..." WB Confidential "] makes use [ndosi] of both internal and external personnel of two other companies: Agic Technology S.r.l. and A1Tech S.r.l. ";

- "A1Tech carries out system management activities of the IT infrastructure of the service offered to AdB, while Agic Technology mainly carries out maintenance and specialist assistance on the application", specifying that "none of the aforementioned companies has been designated sub-processor that AiComply performs on behalf of AdB ";

- the "WB Confidential" application "was designed, starting around 2010, for the acquisition and management of reports of illegal conduct by public entities and financial institutions. The actual marketing of the application took place starting from around 2015 ";

- "the application is made available in its standard version but, at the request of customers, it can be customized by defining, for example, a different classification of the processing status of the reports and the types of behaviors that can be reported as well as enabling not only nominative reports, but also anonymous ";

- with regard to the processing carried out on behalf of the Company, "the reports are managed by one or more subjects of the client who are assigned an authorization profile called" Manager "which allows them to receive the reports, to process them, to interact with the whistleblowers through the application, to change the processing status of the reports as well as to close and, if necessary, to reopen the reports ", highlighting that" the application provides for an additional authorization profile called "System Administrator" to which the maximum administrative privileges for the management and configuration of the application. The subjects to whom this authorization profile is assigned can carry out any operation ";

- "Persons with the authorization profile of" Manager "do not have the privileges to delete the reports on the application, even if their processing is completed. This operation can be carried out, at the explicit request of the customer, with a completely exceptional manual procedure, performed by subjects with the "System Administrator" profile ", specifying that" the cancellation of a report is not allowed by default but requires a temporary disabling this limitation. After carrying out this operation, it is possible to manually delete the data present in three separate tables containing the report, the data of the reporting party and the coupling data of one to the other. However, this cancellation is not definitive as the reports thus canceled merge into a so-called "Trash" for a period of additional thirty days, at the end of which the reports are automatically permanently deleted ";

- "the application is displayed on the public network and that the reachability of the individual instances of the same reserved for the acquisition and management of the reports pertaining to each customer (data controller) is limited only to public IP addresses communicated by each customer. With reference to the application instance reserved for AdB, [...] it can be reached from any IP address to satisfy the specific AdB request to allow the sending of reports outside the company intranet, even by others subjects, stakeholders, external to the same ";

- "the instances of the WB Confidential application use the http (hypertext transfer protocol) protocol for data network transmission", specifying that "specific initiatives are underway to migrate the current application instances from the http protocol to the https protocol" ;

- with regard to the use of cryptographic tools for the storage of reports, "the data stored in the database is not encrypted".

With a subsequent note of the twentieth, the Company provided "a copy of the log files generated by the firewall systems - which allow browsing the internet, accessing the company network - relating to accesses made to the WB Confidential application, from 1 February to 15 April 2019 ", highlighting how" the extraction did not find any log entries prior to February 1, 2019 ". With the same note, additional information and documentation were provided relating to the additional interventions carried out in order to "enhance the security measures adopted to protect the rights and freedoms of the interested parties [... and] to guarantee the protection of the identity of the reporting subjects unlawful conduct ", including, in particular:

- the modification of the "configuration of your firewall, in order to provide for a specific rule for traffic destined for the WB Confidential server" (see technical report attached to the note of XX);
- "enabling a secure data transmission protocol (SSL certificate) to and from the WB Confidential platform";
- "the implementation of a new functionality of the WB Confidential platform [...] which allows the Report Manager to archive the reports" which in this way will no longer be "visible to the Manager, although they can be recovered by means of specific intervention by the AiComply s.r.l. system, at the request of the same Manager ".

With a note of the XX (prot. No. XX, the Office, on the basis of the elements acquired, notified the Company, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions referred to in art.58, par. 2, of the Regulation, inviting the aforementioned data controller to produce defensive writings or documents to the Guarantor or to ask to be heard by the Authority (art.166, paragraphs 6 and 7, of the Code; as well as art.18, paragraph 1, of law no.689 of 24 November 1981).

With the aforementioned note, the Office found that the Company has put in place the processing of personal data of employees and other interested parties, through the use of the application for the acquisition and management of illegal reports, in a manner that does not comply with the principles of "integrity and confidentiality", of "data protection by design" and "data protection by default", in violation of Articles 5, par. 1, lett. f), and 25 of the Regulations; in the absence of appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the processing, in violation of art. 32 of the Regulation; not having carried out an impact assessment on data protection, in violation of art. 35 of the Regulation.

With a note of the twentieth century, the holder sent his defense briefs, "expressing [...] the will to cooperate with [... the] Authority in order to remove the alleged defects", attaching the necessary documentation to prove the measures for this

purpose adopted with regard to the treatments in progress against the generality of employees, and specifying, among other things, that:

- "The growth trend, recorded in the last decade, has unfortunately been abruptly halted by the dramatic effects produced on the aviation sector by the worldwide spread of the SARS-COVID-19 virus. The crisis that has arisen does not, in fact, have any historical precedent […]. The data of these first months of 2021 are certainly no longer reassuring in terms of recovery […]. Also from an economic point of view, AdB's revenues and results decreased significantly, suffering the collapse of traffic and the dramatic situation of airlines and airports […] ";
- "As of May 25, 2018, the legal scenario of reference was anything but mature and well defined. Pending the legislative evolutions that have - gradually - followed one another over time up to today, AdB in April 2019 was [...] to have put in place [...] the necessary formalities for compliance with the principles of the legislation and in line with the methods envisaged by the implementing regulations in force at the time ";
- "in April 2019 [...] we were still in a period of first implementation of the legislation and that most of the [...] clarifying interventions are subsequent to this period and to the specific period of the inspection conducted at the airport, as , ex pluris, in the case of the intervention of the Guarantor Authority with provision of 4 December 2019 n. 9215763 in relation to Wistleblowing treatments. On the other hand, the assessments that the owners and managers were required to make in light of the principles referred to by the legislation remained valid (eg art. 35 GDPR and WP no. 248 of 4 April 2017) and from a risk-based perspective ";
- “AdB immediately took steps to put in place the obligations […]. The pro-activity of AdB [...] should be positively assessed in the general context of the disputes, as it represents on the one hand the strong will of AdB to collaborate in a constructive and improving perspective on the issues described and on the other, it demonstrates good faith about the implementation of complex regulatory requirements in a historical-legal era that is premature from some points of view and, without a doubt, in the settling phase for companies that, like AdB, have their typical characteristics of the sector. [...] ";
- "on XX it communicated to the Guarantor Authority that it had carried out the impact assessment and adopted the technical and organizational measures [...]. The inspections by the Guarantor Authority also represent a moment of confrontation with the Owner and, especially in a period of regulatory uncertainty or with few [...] jurisprudential precedents, they can - and so it was for AdB - support the same owners or managers to put solid legal bases to a management model built according to the

principles of good faith and ordinary diligence, as well as to improve the technical and organizational measures adopted on the basis of risk analyzes conducted on the basis of the reference legislative and regulatory elements. This should not be evaluated by the Guarantor with disfavour, on the contrary, it should be an element of positive consideration of a collaborative attitude such as that demonstrated by AdB and constructive, according to the same principle of the Controller's accountability, for a legal discipline applicable to the specific context. ";

- "aware of the market guidelines that suggest the implementation of a protocol for secure https communication, in relation to the" WB Confidential "application, AdB has evaluated to use the simple http protocol for various reasons, highlighted by the risk analysis for the rights and freedoms of the interested parties and to protect the anonymity of the whistleblower, based above all on the following elements: a. Service active from 2015 to 2019 which received 3 reports (none of which in the period 25/05/2018 - 16/04/2019), thus generating very few transactions with a very low volume of traffic, however extremely complex to identify in the middle of all the electronic traffic that transits on the AdB network, […]; b. Little use for unauthorized suppliers or third parties who wish to take malicious actions on the AdB network in order to obtain useful information or to further propagate abusive access to systems; c. Extremely low probability of threats such as phishing, or other similar threats, defused by the ability to verify the authenticity of the site. Not only would the redemption (number of possible victims who deceive turn into real victims) of e-mails aimed at connecting possible users to the site would be low, but the AdB users actually active are of only one Internal Audit Manager user, extremely aware of the use of the tool ";

- "during the activation phase of the service, the supplier aiComply was asked to provide an evaluation of the merit of the opportunity to activate the https protocol based on their commercial experience and greater knowledge of the state of the art as well as of the general market trend on such systems […]. However, at the suggestion of the supplier and considering the reassurance provided on the subject, the same did not consider such supplementary measures necessary, […]. Without prejudice to the risk analysis carried out in accordance with the obligations imposed on the Data Controller, AdB has relied on the competence and reliability of the supplier [...] ";

- following the inspection "AdB [...] has re-evaluated the analysis and adopted the https tool within 10 days of the inspection, so this measure is effective from 16 April 2019 [...]";

- "in relation to the alleged lack of encryption protocols for the information stored in the database, also in this case it must also be pointed out that at the time of adopting the" WB Confidential "platform, the interpretation of the laws and regulations in force

had not led the Data Controller to recognize a need to adopt the measure of cryptography, as it is applicable and adequate in the cases of cases characterized by large volumes of data and / or in different subjective areas [...] ";

- "Access to the database was precluded to all technical personnel and not AdB and reserved exclusively for the technicians appointed by the aiComply supplier, who had no interest in consulting such data or in communicating or disseminating them";

- "The implementation of this feature required the purchase of an additional feature [...]. This amount would have been a reasonably disproportionate implementation cost compared to [… the overall cost of the service] ";

- "Any access by unauthorized third parties would have occurred in any case with respect to a system containing 3 reports between 2015 and 2019, scarcely usable both for economic purposes (eg. Request for redemption or resale on the market), and for the purpose of perpetrating further attacks on AdB or other stakeholders part of its ecosystem ";

- "For the sake of completeness of information, it should be noted that the supplier aiComply has in the meantime proposed to AdB, following the transfer of their services to the Microsoft Azure cloud platform, the adoption of an appropriate and sustainable encryption methodology for the writer, also in consideration of implementation costs, especially in an unprecedented crisis situation in the aviation sector and employees on layoffs. This technical solution could, therefore, be implemented from the current year, if the supply contract with the current supplier is renewed ";

- “while confirming that for the purposes of preventing attacks and monitoring the network, the firewalls kept track of the access information to the“ WB Confidential ”platform in the logs, the following elements should be noted: a. These logs prevent you from knowing what action was taken on the platform (eg distinguish who downloaded the manual or who made an anonymous or nominative report or who only read the privacy policy). b. These logs are so small in number that they require storage over a long period, a specific analysis in order to identify, among all the logs, those specific to access "WB confidential", an operation that can only be done by someone who knows the platform in particular; as regards the risks associated with collaborators, suppliers or unauthorized third parties, reference is made to point 1 and to all the analyzes carried out on the risks represented by these actors as well as on the countermeasures in place. The analysis made, therefore, shows how, even in 2015, when the GDPR was not in force and in 2018 after its applicability, the principles of data protection by design and by default were respected in compliance with Article 25. With the same spirit of collaboration and enrichment of the methodology in use, it should be noted that AdB has configured [... a new] technical and organizational measure ", configuring the firewall systems so as not to record in the logs the traffic destined for the" WB Confidential ";

- "in the context of the risk analysis he noted the need to carry out the impact assessment pursuant to art. 35 GDPR in relation to the processing [… in question…]. Well, considering the small number of data processed and the data subjects involved in the processing in question, also considering that among the criteria indicated by WP29 no. 248 of 4 April 2017, only one of these is fully existing (the vulnerability of the subjects involved in the treatment), AdB considered the treatment with a "not high" degree of risk and, for this reason, considered it unnecessary to proceed with the assessment of impact since 25 May 2018, but to monitor the risk underlying the treatment in question and the progress of the treatment and reassess it when updating the register (annually). [...] ";

- “the assessment of the above criteria guided AdB in detecting the risk underlying the treatment, not so much with reference to the necessity of carrying out the DPIA […], but with reference to the need to carry it out with priority over other treatments. Consequently, in the choices and evaluations of AdB the sensitivity of the treatment was in any case taken into account, in general, however, since in principle, the same WP29 believes that the greater the number of criteria satisfied by a given treatment, the greater the number of criteria satisfied by a given treatment, the the greater the likelihood that it presents a high risk to the rights and freedoms of the data subjects and, therefore, that a DPIA is required regardless of the measures that the holder plans to take. In other words, without prejudice to the foregoing, the [...] Authority is asked to reassess the complaint made in relation to the violation of art. 35 GDPR, as as described AdB had carried out all the necessary assessments in compliance with art. 35 GDPR and in compliance with the indications prescribed by WP29 and to take into account the planning carried out according to a logic of riskiness relating to the treatment in question for the purposes of the complete execution of the obligations provided for by the law. This is also demonstrated by the proactivity with which AdB has [...] in close coordination with the Guarantor Authority has put in place the DPIA [...] ".

The hearing requested by the Company was also held on April 16, 2021, pursuant to art. 166, paragraph 6, of the Code, on the occasion of which, in confirming what has already been declared in the defense briefs, it was represented, among other things, that:

- "the Company has always approached the subject of personal data protection with great attention, adopting new technologies, adopting a privacy organizational model and carrying out, among other things, a risk analysis with regard to the various treatments carried out";

- "the Company's level of compliance was also highlighted during the inspections, following which the Company proactively

intended to adopt, in the days immediately following the aforementioned assessments, a series of further technical measures aimed at further raising the level of compliance with the provisions of the Regulation and the Code and carrying out an impact assessment on data protection for processing related to whistleblowing ";

- “the Company has demonstrated that it has adopted an approach based on the principle of data protection by design, which has also been applied to processing relating to whistleblowing, for which an assessment of the potential and actual risks for the parties concerned was carried out; evaluation that took into account the small number of whistleblowing reports acquired and processed, the limited number of interested parties involved, the categories of personal data processed (which did not include data belonging to particular categories) as well as the reference context, also with regard to technological solutions at the time available on the market and in the general reference application framework ";

- "the choices adopted by the Company regarding the protection of personal data have always been inspired by compliance with the principles of proportionality, necessity and lawfulness of processing".

3. Outcome of the preliminary investigation.

The regulations on the protection of employees who report offenses and the regulations on the protection of personal data (so-called whistleblowing) - originally envisaged only for public entities (see Article 54-bis of Legislative Decree 30 March 2001, 165, introduced by Article 1, paragraph 51, of Law No. 190/2012) - was supplemented and amended by Law no. 30 November 2017, n. 179 ("Provisions for the protection of the authors of reports of crimes or irregularities of which they have become aware in the context of a public or private employment relationship"), which introduced a new discipline on whistleblowing referred to private subjects, integrating the legislation on "administrative liability of legal persons, companies and associations even without legal personality" (see Article 2 of Law No. 179/2017 which added paragraph 2-bis to Article 6 of Legislative Decree .lgs. 8 June 2001, n. 231).

The aforementioned regulatory framework provides, more generally, measures aimed at protecting the disclosure of the identity of the whistleblower, in order to mainly prevent the adoption of discriminatory measures against the same.

In this context, the processing of personal data carried out by the obliged subjects can be considered necessary to fulfill a legal obligation to which the data controller is subject (articles 6, paragraph 1, letter c), 9, par. 2, lett. b), and 10 of the Regulation).

For these reasons, the aforementioned sector regulations, which provide for the processing of employee data reporting offenses, must be considered as one of the "most specific rules to ensure the protection of rights and freedoms with regard to

the processing of personal data of employees in the context of employment relationships ”provided for by art. 88, par. 1, of the Regulation (see provision of 4 December 2019, web doc. No. 9215763, opinion of the Guarantor on the outline of "Guidelines for the protection of the authors of reports of crimes or irregularities of which they have become aware due to an employment relationship, pursuant to Article 54-bis of Legislative Decree 165/2001 (so-called whistleblowing) "of ANAC).

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 the data must also be "processed in such a way as to guarantee adequate security" of the same, "including the protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage "(art. 5, par. 1, lett. f), of the Regulation).

The owner, in the context of the necessary identification of the technical and organizational measures suitable to guarantee a level of security adequate to the specific risks deriving from the treatments in question (articles 24, 25 and 32 of the Regulation), may resort to a person responsible for the performance of some processing activities to which it gives specific instructions (cons. 81, articles 4, point 8), and 28 of the Regulation) and must define its own reporting management model in compliance with the principles of "data protection by design" and of “protection by default”, also taking into account the observations presented in this regard by the data protection officer (DPO).

3.1. Failure to use cryptographic techniques for the transport and storage of data

During the investigation it emerged that access to the "WB Confidential" application for the acquisition and management of reports of offenses took place via the http protocol (hypertext transfer protocol), that is a network protocol that does not guarantee integrity and confidentiality of the data exchanged between the user's browser and the server hosting the application in question, and does not allow users to verify the authenticity of the website with which they are interacting.

In this regard, taking into account the nature of the data exchanged and the high risks deriving from their possible acquisition by third parties, it is believed that the method of accessing the application in question cannot be considered a suitable measure to guarantee an adequate level of security. .

Although, during the investigation, the Company indicated that it did not initially consider it necessary to adopt a secure network protocol (such as the https protocol) based on the assurances of the Supplier and due to the limited number of reports received ("Very few transactions with a very low volume of traffic"), the "little use", for any third parties, of the information contained in the reports acquired through the application and the "extremely low probability of threats such as phishing [...]

defused by the possibility of verifying the authenticity of the site ", it is noted that, in any case, the data controller must implement adequate technical and organizational measures taking into account the state of the art, the implementation costs, the nature, the scope of application, the context, purposes and risks associated with the processing.

With reference to the retention of data relating to reports acquired through the "WB Confidential" application, during the investigation it emerged that the same does not provide for the encryption of personal data (identification data of the whistleblower, information relating to the report and any attached documentation ) stored in its database. This measure had been recommended by ANAC since 2015 in relation to the acquisition and management of reports of illegal conduct (see the recommendations on the use of "end-to-end encryption tools for the contents of the reports and any attached documentation ", Guidelines on the protection of public employees who report offenses (so-called whistleblower), adopted with resolution no. 6 of 28 April 2015).

In this regard, the Company has represented, among other things, that it originally considered that it did not have to "adopt the measure of encryption, as it is applicable and adequate in cases characterized by large volumes of data and / or in different subjective areas", since "access to the database [... was] reserved exclusively for the technicians appointed by the supplier aiComply, who had no interest in consulting such data or in communicating or disseminating them" and as "the implementation of this functionality required the purchase of an additional functionality [… with] an implementation cost that is reasonably disproportionate to [the overall cost of the service] ".

The defensive arguments of the Company, in relation to the failure to adopt measures for the encryption of data both in transport and in storage, although taken into due consideration for the purposes of this provision, are however not sufficient to completely exclude the responsibility of the data controller with regarding the obligations deriving from the regulations on the protection of personal data (see articles 24 and 32 of the Regulation). This is also due to the fact that the owner is the subject on whom the decisions regarding the purposes and methods of processing the personal data of the interested parties fall and who has a "general responsibility" on the treatments put in place (see art. 5, par. 2, so-called principle of "accountability", and 24 of the Regulation), also with reference to the preparation of technical and organizational measures that meet the requirements of the Regulation in terms of safety (articles 24 and 32 of the Regulation), even when certain processing operations are carried out by a manager on their behalf (see the recent decisions of the Guarantor also relating to the role and related responsibilities of the data controller and data processor, provisions of September 17, 2020, nos. 160 and 161, web

doc. no. 9461168 and 9461321, provision 11 February 2021, no. 49, web document no. 9562852, as well as provision 17 December 2020, no. 280, 281 and 282, web document no. 9524175, 9525315 and 9525337).

For these reasons, the failure to use cryptographic tools for the transport and storage of data does not comply with the provisions of art. 5, par. 1, lett. f), and art. 32 of the Regulation which, in its par. 1, lett. a), expressly identifies encryption as one of the possible security measures suitable for guaranteeing a level of security appropriate to the risk (see also cons. 83 of the Regulation in the part in which it provides that "the data controller [...] should evaluate the risks inherent to the processing and implement measures to limit these risks, such as encryption ").

Furthermore, it is noted that, based on the principle of "data protection by design" (Article 25, paragraph 1, of the Regulation), the data controller must adopt adequate technical and organizational measures to implement the principles of protection of data (Article 5 of the Regulation) and must integrate in the processing the necessary guarantees to meet the requirements of the Regulation and protect the rights and freedoms of the data subjects. This obligation also extends to treatments carried out by means of a data controller. In fact, the processing operations carried out by a manager should be regularly examined and evaluated by the owner to ensure that they continue to comply with the principles and allow the owner to fulfill the obligations established by the Regulation (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 7 and 39). Therefore, the failure to adopt the aforementioned measures - aimed at implementing the principles of data protection and integrating the necessary guarantees in the processing in order to meet the requirements of the Regulation - is also in contrast with the principle of "data protection by design "Pursuant to art. 25, par. 1, of the Regulation.

For these reasons it is concluded that, until the adoption of the new measures with which the Company has ensured the protection of data both in the transport and in the storage phase, the processing carried out through the application in question is occurred in violation of Articles 5, par. 1, lett. f), 25, par. 1, and 32 of the Regulation.

3.2. Tracking of accesses to the "WB Confidential" application.

During the investigation it was found that access to the "WB Confidential" application by the Company's employees with workstations or personal devices connected to the company network was mediated by "new generation firewalls, which allow you to configure specific rules for surfing the Internet, also due to the role of the various functions and duties performed by individual employees ". These devices "stores [go] ng in specific log files the navigation operations carried out, the retention

period of which is set at 90 days", including the connections to the "WB Confidential" application.

As is clear from the documentation acquired during the inspections, the logs generated by the aforementioned firewall devices contained, among others, the IP address of the device used to connect to the "WB Confidential" application and, "by virtue of the integration of the firewall with Active Directory ", the username of the person who was making this connection.

In this regard, the Company specified that in the aforementioned logs there are no "information about specific accesses to the various sections of the site (.aspx pages), so it is not possible to know which specific page has been accessed (eg. Anonymous report, reporting by name, FAQ, Regulations, ...) ", highlighting that" given the information generated and stored by the firewall and the specific skills on the functioning of the components of the platform owned by the Owner, it is highly unlikely, if not "impossible", to identify any visitors who may report "(see technical report attached to the note of the XX, p. 4).

In acknowledging that "for greater prudence and to guarantee the protection of the identity of the whistleblower, [... the Company] considered it appropriate to have the configuration of its firewall changed, in order to provide for a specific rule for traffic destined for the WB Confidential server" and that "the new rule, effective from 15.04.2019 requires that no log information be generated for all direct accesses to the WB Confidential platform" (see technical report attached to the note of XX, p. 4), it is noted, however, that, contrary to what the Company claims, the recording and storage, in the logs of the firewall devices, of the information relating to the connections to the "WB Confidential" application could have allowed the traceability of the subjects who used the application, including the reporting persons. This, considering precisely the small number of connections to the application in question, which therefore rendered the other measures adopted to protect the confidentiality of the identity of the reporting persons as required by the sector regulations ineffective, placing itself in contrast with the provisions referred to in art. 5, par. 1, lett. f), and art. 32 of the Regulation.

In this regard, for the purposes of the overall assessment of compliance with the processing security obligations, the information highlighted by the Company regarding the fact that the logs did not allow to know the specific action performed by users on the application and that a "Specific analysis in order to identify, among all the logs, those specific to access" WB confidential "".

In this framework, moreover, the data controller, in addition to respecting the principle of "data protection by design" (Article 25, paragraph 1, of the Regulation) - adopting technical and organizational measures adequate to implement the protection principles of the data (art. 5 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 - must also, in compliance with the principle of "data protection by default" (art . 25, par. 2, of the Regulation), make choices that ensure that, by default, only the processing strictly necessary to achieve a specific and lawful purpose is carried out. This therefore implies that, by default, the data controller must not collect personal data that are not necessary for the specific purpose of the processing (see "Guidelines 4/2019 on article 25 Data protection by design and by setting default ", adopted on 20 October 2020 by the European Data Protection Board, spec. points 42, 44 and 49).

As recently highlighted by the Guarantor (see, in particular, with regard to the processing of user and employee data through a service booking system at the counter, provision no. 282 of 17 December 2020, web doc. No. 9525337 , but already provision. 7 March 2019, n.81, web doc. n.9121890), the data controller, even when using products or services made by third parties, must verify, also with the support of the data protection officer where appointed, compliance with the principles applicable to data processing (Article 5 of the Regulation) by adopting, in compliance with the principle of accountability, the appropriate technical and organizational measures and giving the necessary instructions to the service provider (see Articles 5, par . 2, 24, 25 and 32 of the Regulation).

In this perspective, the data controller must carry out a risk assessment and make sure that the functions that do not have a legal basis, are not compatible with the purposes of the processing, or are in contrast with specific sector regulations provided for by the legal system (see, in particular, the discipline on whistleblowing, but also the national and higher protection laws for data subjects with regard to processing in the workplace, Article 88 of the Regulation in relation to Articles 113 and 114 of the Code ; from this last point of view, with regard to tracking operations of connections to Internet sites by employees, see most recently provision no. 190 of 13 May 2021, currently being published).

Failure to adopt the necessary measures to protect data subjects with regard to tracing access to the "WB Confidential" application is therefore also in contrast with the principles of "data protection by design" and "data protection by default" "Pursuant to art. 25 of the Regulation.

For these reasons, it is believed that the registration and storage, within the logs of the firewall devices, of information directly identifying the users of the "WB Confidential" application has been put in place, up to the moment in which the Company has provided to adopt specific measures to protect the interested parties aimed at no longer recording access to the application in question in the logs of the firewall systems, in violation of Articles 5, par. 1, lett. f), 25 and 32 of the Regulations.

3.3. Failure to perform a data protection impact assessment.

As is clear from the preliminary evidence in the documents, the processing of the personal data of the data subjects was carried out in the absence of a preliminary impact assessment on data protection due to "the small number of data processed and the data subjects involved in the processing in question" (see minutes 2 April 2019, p. 2).

In this regard, it is believed that the processing of personal data through the systems for acquiring and managing reports of alleged illegal conduct - due to the particular sensitivity of the information processed, as well as the high risks, in terms of possible retaliatory and discriminatory effects, including indirect ones , for the whistleblower, whose identity is protected by a specific guarantee and confidentiality regime provided for by sector legislation (both at national and European level, see, lastly, Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons reporting violations of Union law) - present specific risks to the rights and freedoms of data subjects.

This, also considered, the "vulnerability" of the data subjects (reporting and reported subjects) in the workplace (see articles 35 and 88, paragraph 2, of the Regulation; "Guidelines concerning the impact assessment on data protection as well as criteria to establish whether a treatment "may present a high risk" pursuant to Regulation 2016/679 ", WP 248 of 4 April 2017; see, most recently, provision of 4 December 2019, web doc. no. 9215763, with the which the Guarantor has given the opinion to ANAC on the outline of "Guidelines for the protection of the authors of reports of crimes or irregularities of which they have become aware due to an employment relationship, pursuant to art. 54-bis of Legislative Decree 165/2001 (so-called whistleblowing) ", where express reference is made to" the main obligations provided for by the legislation on the protection of personal data (articles 13, 14, 30, 35 and 36 of the Regulation), also taking into account the specific risks to the rights and freedoms of those concerned ti in the workplace ").

In acknowledging that, following the investigations carried out by the Company, the same carried out, albeit belatedly, an impact assessment on data protection pursuant to art. 35 of the Regulation (see note of XX, p. 1, and attached "Privacy Impact Assessment") it must be concluded that, in any case, up to the date of preparation of the same (April 2019), the processing was carried out in the absence of a impact assessment necessary to identify specific measures to mitigate the risks deriving from the processing, in violation of art. 35 of the Regulation. However, taking into account the first application phase of the Regulation and the Code in which the processing subject of this investigation took place, the uncertainties deriving from the evolving legal framework, and the fact that specific clarifications on the point were provided by the Guarantor in the context of

of the aforementioned opinion delivered to ANAC on 4 December 2019, i.e. after carrying out the inspections at the Company, it is believed not to have to proceed, on this point, with the application of an administrative sanction, also pursuant to art. 22, paragraph 13, of Legislative Decree 10 August 2018, n. 101.

4. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the data controller in the defensive writings □ the truthfulness of which one may be called to answer pursuant to art. 168 of the Code □ although worthy of consideration and indicative of the full collaboration of the data controller in order to mitigate the risks of the processing, compared to the situation present at the time of the investigation, they do not however allow to overcome the findings notified by the Office with the act of initiation of the procedure and are therefore insufficient to allow the filing of this proceeding, since none of the cases provided for by art. 11 of the Guarantor Regulation n. 1/2019.

In order to determine the applicable law, in terms of time, the principle of legality referred to in art. 1, paragraph 2, of the l. n. 689/1981, according to which the laws that provide for administrative sanctions are applied only in the cases and times considered in them. This determines the obligation to take into account the provisions in force at the time of the committed violation, which in the case in question - given the permanent nature of the alleged offenses - must be identified in the act of cessation of the unlawful conduct. In acknowledging that the data controller has, during the investigation, taken steps to conform the treatment to the principles of the Regulation, to adopt appropriate technical and organizational measures to guarantee a level of security adequate to the risk presented by the treatment, as well as to carry out a specific impact assessment on data protection, it is believed that, given the cessation of unlawful processing occurred after the date on which the Regulation became applicable (see note of the XX, in which account is taken of the various initiatives taken by the owner to remedy the alleged violations), the Regulation and the Code constitute the legislation in the light of which to evaluate the treatments in question.

The preliminary assessments of the Office are therefore confirmed and the unlawfulness of the processing of personal data carried out by the Company is noted as it occurred in a manner that did not comply with the general principles of "data protection by design" and "data protection by default ", in violation of Articles 5, par. 1, lett. f), 25, 32 and 35 of the Regulation.

The violation of the aforementioned provisions also makes the administrative sanction applicable pursuant to art. 58, par. 2, lett. i), and 83, para. 4 and 5, of the Regulation.

In this context, considering that the conduct has exhausted its effects, the conditions for the adoption of corrective measures, pursuant to art. 58, par. 2, of the Regulation.

5. Adoption of the injunction order for the application of the pecuniary administrative sanction and ancillary sanctions (Articles 58, paragraph 2, letter i), and 83 of the Regulations; 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 Regulations, in this case 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.

For the purposes of applying the sanction, the nature, object and purpose of the processing were considered, the sector discipline of which provides, to protect the interested party, a high degree of confidentiality with specific regard to the identity of the same.

On the other hand, it was considered that the processing involved, in practice, a small number of data subjects (between reported and reporting subjects) due to the limited number of reports present in the application used for the acquisition and management of reports of conduct illicit. In addition, the data controller has provided a particular collaboration during the investigation by adopting, already following the inspection activity conducted by the Office and with the help of the data protection officer, technical and organizational measures aimed at conforming the treatments in progress to the regulations on the protection of personal data, in compliance with the principle of accountability. The economic repercussions on the sector in which the data controller operates due to the worldwide spread of the SARS-CoV-2 virus were also taken into consideration.

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

On the basis of the aforementioned elements, evaluated as a whole, it is considered to determine the amount of the financial penalty, in the amount of € 40,000.00 (forty thousand) for the violation of Articles 5, par. 1, lett. f), 25 and 32 of the Regulation.

In quantifying the sanction, the Guarantor held the phase of first application of the sanctioning provisions, pursuant to art. 22, paragraph 13, of the d. lgs. 10 August 2018, n. 101, with particular regard to the violation of art. 35 of the Regulation.

Taking into account the particular delicacy of the illegally processed data, 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 by art. 16 of the Guarantor Regulation n. 1/2019.

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

WHEREAS, THE GUARANTOR

detects the unlawfulness of the processing carried out by Aeroporto Guglielmo Marconi di Bologna S.p.a. for the violation of articles 5, par. 1, lett. f), 25, 32 and 35 of the Regulations, within the terms set out in the motivation;

ORDER

at Aeroporto Guglielmo Marconi di Bologna S.p.a., in the person of the pro-tempore legal representative, with registered office in Bologna, via Triumvirato, n. 84, C.F./P.IVA 03145140376, pursuant to art. 58, par. 2, lett. i), and 83, par. 5, of the Regulations, to pay the sum of € 40,000.00 (forty 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 Guglielmo Marconi Airport of Bologna S.p.a. to pay the sum of € 40,000.00 (forty 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;

HAS

the publication of this provision on the website of the Guarantor pursuant to art. 166, paragraph 7, of the Code;

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, of art. 152 of the Code and 10 of the legislative decree 1 September 2011, n. 150, 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, June 10, 2021

PRESIDENT

Stanzione

THE RAPPORTEUR

Cerrina Feroni

THE SECRETARY GENERAL

Mattei