- SEE ALSO NEWSLETTER OF 2 AUGUST 2021

[doc. web n. 9685947]

Order injunction against aiComply S.r.l. - June 10, 2021

Record of measures

n. 236 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 Dr. Agostino Ghiglia;

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.

As a result of the complex 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:

- AdB - publicly held joint stock company for about 45% of the share capital and listed on regulated markets, the only operator of Bologna airport, as public service concessionaire until 28 December 2044 by virtue of an agreement with the National Civil Aviation Authority (ENAC) - has 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 Company in SaaS (Software as a Service) mode, for the acquisition and management of reports of illegal conduct. To this end, the relationship with the Company, as data processor, has been regulated pursuant to art. 28 of the Regulations (see minutes of the XXth, spec. Annex 10 - designation deed);
- "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);

- AdB "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);

- 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 AdB has on the point represented that it has initiated evaluations about "the opportunity to act such measure to guarantee the confidentiality and integrity of the data transmitted on the public network "(see minutes of

the XX, p. 3).

During the investigations carried out at aiComply (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 activities 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".

During the investigations, it was possible to verify that the user with the "System Administrator" profile used by the Company for accessing the "WB Confidential" application of AdB was shared between two subjects authorized for processing.

With a subsequent note of the twentieth, AdB 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 with regard to the profiles relevant to this investigation:

- "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 measures referred to in art. 58, par. 2, of

the Regulations, inviting the aforementioned data controller 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 law no. 689 of 24 November 1981).

With the aforementioned note, the Office found that the Company has carried out the processing of personal data without having regulated the relationship with the subjects operating as sub-processors, in violation of art. 28 of the Regulation, as well as in the absence of appropriate technical and organizational measures to ensure an adequate level of security for the risks presented by the processing, in violation of art. 32 of the Regulation.

With a note dated the XXth, the Company sent its defense briefs, declaring, among other things, that:

- "at the time of carrying out the inspection activities (dating back almost two years ago) the representatives of the Guarantor carried out the investigations with reference to what at the time was a mere production environment of the Application licensed to Aeroporti di Bologna: they were there were only five reports, of which two were real and three were test ";
- the Authority "proceeding to the dispute tout court of the violation of Article 32 of the Regulation for not having adopted the Company suitable security measures with particular reference to https protocols and cryptography in data retention: 1. did not take into account the nature of the processing carried out by the Company on the date of the inspection (extraordinarily limited processing of purely personal data and with the absence of information of a particular nature, referring only to two real reports subject to conservation through the Application); 2. did not take into account the scope and context of the processing through the Application ascertained on 10 April 2019 (with data being processed in the context of mere testing and production of the IT environment that was the subject of the inspections) ; 3. did not take into account - in its assessments regarding the initiation of the sanctioning procedure - "the risk of varying probability and severity" which certainly appears probabilistically very close to zero if only the treatments limited to the date of the inspection are evaluated (and not to mention that to date and for all users of the Application - not only Aeroporti di Bologna - there has never been any accidental or illegal destruction, loss, modification, disclosure, unauthorized access to personal data transmitted, stored or otherwise processed from the Application, nor any material or immaterial damage to any interested party ";
- "the security measures indicated in article 32 of the GDPR do not constitute a generalized legal obligation which - if these measures are omitted - leads to the initiation of a sanctioning procedure against the data controller / manager almost automatically and on the basis of the mere and verified lack of the catalog of security measures indicated therein in paragraph

2. It is the legislator himself who prescribes that these measures (including data encryption and the resilience and integrity of the processing services that concern here) must be adopted by the Data Controller or by the Responsible for the treatment "where appropriate". If it were admitted - as it seems in fact to believe this esteemed Authority in its administrative provision of contestation of violation and initiation of the sanctioning procedure - that the data controller / manager must always and in any case adopt (in any case and not where appropriate) the measures of security indicated in article 32 of the GDPR - even in cases of processing such as those contested by the Company in the extension, modalities and limitations referred to in the assessments of 10 April 2019 - the consequence of an abnormal application of article 32, paragraphs 1 and 2, RGPD which would in fact be transformed into a mandatory mandatory rule as regards the catalog of security measures to be adopted ";

- "this appears relevant with regard to the consequences also in light of the provisions of article 3, paragraph 1, of Law 241/1990 [... which] requires that every administrative measure must be motivated and that" the motivation must indicate the conditions for fact and legal reasons that determined the administration's decision, in relation to the results of the investigation "";

- "This esteemed Authority considered at the outcome of the investigation that it had to contest (without adequately motivating) that without any doubt the only security measures compliant with the situation subject to the inspection assessment would have been the encryption of the (very limited) personal data processed in the 'Application test and production environment as well as the availability of the Application as SaaS on a public network with the https protocol instead of the http protocol (which in any case is not automatically insecure, also in light of the evaluations and parameters mentioned above with respect to the specificity of the context)";

- "The server on which the Application runs is exposed on the Internet only to ports 80 and 443 (http and https) open in the firewall. But, on the other hand, no other services are displayed on the public line. Furthermore, the server is in DMZ (delimitarized zone or demilitarized zone, which in computer science indicates a computer network that acts between two networks as a buffer zone with its own IP address and delimits them by means of strict access rules) with a firewall that protects the DMZ area of the public network. Access is allowed only from internal network and nominal VPN (Virtual Private Network), through the http and https ports and through the Remote Desktop Protocol (RDP) which, as it is known, is the proprietary protocol of Microsoft Inc. based on data encryption 128 bits through the RC4 algorithm, which implements advanced secure access management mechanisms ";

- "the server cannot surf the Internet, has all outgoing ports disabled (except for those towards the Company's internal LAN, to ensure correct functioning) and to directly access the database containing the data referred to in the reports managed by 'Application it is necessary to access the server only via RDP protocol, with system administrator credentials ";

- "the Company has also adopted as a security policy that of decoupling the reporting person's data from the information relating to the report (in fact, Aeroporti di Bologna cannot know the personal details of the reporting person, except in cases of specific request as per law)" ;

- "since last year the new version of the Application - among other measures - adopts the https protocol and data encryption among the security options";

- "The set of technical and organizational security prerogatives summarized above and adopted by the Application cannot therefore not converge the assessments in the perspective of Article 32 RGPD on full compliance of the processing services referred to in the Application (already at the date of XX) the regulatory requirements on security ";

- "in the discussions between the Company and Aeroporti di Bologna during the negotiation of the Application supply agreement there was an appropriate exchange of technical documentation designed to allow Aeroporti di Bologna to make every exclusive decision on the security measures to be implemented in the Application ";

- "Aeroporti di Bologna is in any case such a body as to have within it the specific ICT specialist and infrastructural skills to carry out the necessary and exclusive assessments pertaining to the Data Controller as to the security measures that had to be implemented by the Company in the Application ";

- "in the offer (AI / GDG / 15 / 326-4) of the Company to Aeroporti di Bologna the possibility of" implementing confidential protocols for the transport of data (for example SSL) as well as the use of end-to-end encryption for the contents of the reports and any attached documentation ";

- "with the specific supply of the technical documentation referred to in the offer (AI / GDG / 15 / 326-4) of the Company to Aeroporti di Bologna, aiComply S.r.l. has fulfilled its obligation to support and supply specialist skills and technical information to the Aeroporti di Bologna Data Controller in order to allow this body - as recalled by the 7/2020 Guidelines on the role of the Data Processor with respect to its own security decisions only of the Data Controller - to indicate to aiComply their final decisions on security in the Application processing services ";

- "It was a precise economic and contractual choice of Aeroporti di Bologna to indicate to the Company to proceed with the

development of the Application without adopting those specific security measures (and in any case - for the above argued - aiComply S.r.l. has in any case provided a Secure application) with the specific implementation of confidential protocols for the transport of data (for example SSL) as well as the use of end-to-end encryption tools for the contents of the reports and any attached documentation ", having done Bologna a precise choice and taken a precise security decision in the development of the Application exclusively attributable to that Data Controller ";

- "this is all the more confirmed when we read in the provision to initiate the sanctioning procedure notified by this respectable Authority to the Company that" it has been verified that the application, exposed on the Internet, does not use a secure network protocol (such as the https) for the transport of data and this Company (Aeroporti di Bologna n.d.r.) has on the point represented that it has initiated assessments on "the opportunity to implement this measure to guarantee the confidentiality and integrity of data transmitted on the public network" (see minutes of April 2, 2019, p. 3) ";

- "it appears logical and legally founded to conclude that no omissive responsibility or sanctioning consequence - for all the above deduced and argued - is well-founded attributable to the company aiComply S.r.l. for alleged violation of Article 32 of the RGPD sub specie failure to adopt specific security measures within the Application, such as https protocol or data encryption at the time of the inspection ";

- "First of all, it should be remembered that no rule of the RGPD directly prohibits the sharing of users and that pursuant to the combined provisions of articles 5, paragraph 1, letter (f) and 32, paragraph 1, of the RGPD, whether such a practice could prove that does not comply with these rules can only be the result of a precise, thorough and non-automatic application of the principle of "integrity and confidentiality" to be assessed in the light of "the state of the art and the costs of implementation, as well as the nature, 'object, context and purposes of the processing, as well as the risk of varying probability and gravity for the rights and freedoms of individuals ";

- "in other words, it does not appear to comply with the law to automatically associate the verification of the sharing of the single non-nominal user" agicwhistle \ spadmin "with the circumstance that by doing so it would be" possible for an unauthorized person to operate, in the absence of of a specific will of the data controller, in the context of processing systems and services "(see par. 4.2, page 7 of the provision to initiate the procedure)";

- "the agicwhistle \ spadmin user - at the time of the inspection findings - was actually a user shared by the two authorized system administrators of the Company and of the company AGIC Technology S.r.l., however given the fact that: this user was

necessary to administer the platform Microsoft Sharepoint 2010 as a whole, on which the Application is based; it was necessary to carry out installation, administration and maintenance of the entire Microsoft Sharepoint 2010 platform (and not of the single application); it could not be linked to a personal account of a specific system administrator (since the Windows SharePoint 2010 Platform did not have multi-access options at the time) ";

- "also having to consider - pursuant to art. 32, paragraph 1, RGPD - the nature, context and purposes, it emerges that the sharing of the agicwhistle \ spadmin user: 1. has never provided for concurrent accesses by the two administrators; 2. the sharing had only the duration of the test phases and production of the Application; 3. during these phases he was only the system administrator of AGIC Technology S.r.l. to access to provide for interventions in the application of a technical nature carried out exclusively by AGIC Technology S.r.l. itself, in possession of the necessary skills; 4. after the go-live of the Application, the agicwhistle \ spadmin user was used exclusively by the system administrator of aiComply S.r.l., at that point the customer's only interface to receive any requests for intervention; 5. the sharing (only formal and nominative) of the users as detailed above in concrete and the different activities (chronologically out of phase in time) carried out by the two system administrators in any case could not have entailed any "high and unjustified risk for the rights and freedoms of the interested parties "as apodictically represented in the provision of this esteemed Authority";
- "if the general assumption of this esteemed Authority is obviously correct that" the use of non-nominal users, by more than one person, prevents the actions performed in a computer system from being attributed to a specific subject, with prejudice, even for the data controller and the data processor "(see par. 4.2, page 6 of the provision to initiate the procedure), it certainly seems less acceptable to believe that such an impediment could have occurred in the specific case, with only two administrators of system, with different technical and managerial skills, with accesses out of phase over time and for carrying out administration activities that are completely different from each other ";
- "aiComply S.r.l. has appointed AGIC Technology S.r.l. (the two companies are part of the same business group) providing system administration services in general and in relation to the activities that are carried out in house and through inter-company agreements within the companies of the AGIC Group. A1Tech S.r.l. on the other hand, she was appointed as Data Processor and System Administration Service Provider (the related documents are on file) ";
- "with specific reference to the Aeroporti di Bologna contract: 1. aiComply makes use of A1Tech S.r.l., which carries out system management activities of the IT infrastructure of the service offered to Aeroporti di Bologna and in carrying out this

technical activity does not process personal data of any type (and even potentially does not have access to the data), in this case the obligation to appoint a sub-processor is no longer required; 2. the Company makes use of AGIC Technology S.r.l., which mainly carries out maintenance and specialist assistance activities on the Application. AGIC Technology S.r.l., is among the first Microsoft Gold Partners in Italy, with over 150 certified resources. Furthermore, the companies of the AGIC Group have acquired numerous quality certifications (such as ISO 9001: 2015) and are all subject to stringent compliance requirements in the provision of services to customers. It follows that the substantive rationale of Article 28 of the GDPR (responsible and sub-processors who provide sufficient guarantees to implement adequate technical and organizational measures in such a way that the processing meets the requirements of the Regulation and guarantees the protection of the rights of the data subject), beyond the formal omission of the act of appointment as sub-processor, it can be considered prosecuted and evaluated in due perspective for the purposes of this proceeding ".

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 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, including those without legal personality" (see Article 2, 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 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 general, although the data controller, who determines the purposes and methods of data processing, has a "general responsibility" for the treatments put in place (see Article 5, paragraph 2, so-called "accountability", and 24 of the Regulation), even when these are carried out by other subjects "on its behalf" (cons. 81, articles 4, point 8), and 28 of the Regulation), the Regulation has governed the obligations and other forms of cooperation to which the data controller is responsible for and the scope of the related responsibilities (see articles 30, 32, 33, par. 2, 82 and 83 of the Regulation).

The data processor is entitled to process the data of the interested parties "only on the documented instruction of the owner" (Article 28, par. 3, letter a), of the Regulation) and the relationship between the owner and manager is governed by a contract or by another legal act, stipulated in writing which, in addition to mutually binding the two figures, allows the owner to give instructions to the manager also from the point of view of data security and provides, in detail, what the subject matter is governed, the duration, the nature and purposes of the processing, the type of personal data and the categories of data subjects, the obligations and rights of the owner and manager. Furthermore, the data controller must assist the owner in ensuring compliance with the obligations deriving from the data protection regulations, "taking into account the nature of the processing" and the specific regime applicable to the same (Article 28, paragraph 3, letter f), of the Regulation).

In this context, the person in charge may not have recourse to another person in charge "without the prior written, specific or general authorization of the data controller" and, in this case, "the same obligations are imposed on this other data controller [...] in subject of data protection, contained in the contract or other legal act between the controller and the data controller "(Article 28, paragraphs 2 and 4, of the Regulation).

Furthermore, art. 32 of the Regulation establishes that, not only the owner, but also the person in charge of the processing, within the scope of his / her competences and the tasks delegated by the owner, "taking into account the state of the art and the costs of implementation, as well as the nature, 'object of the context and purposes of the processing, as well as of the risk of varying probability and gravity for the rights and freedoms of individuals "implement" adequate technical and organizational measures to ensure a level of security appropriate to the risk "and that "In assessing the adequate level of security, particular account is taken of the risks presented by the processing that derive in particular from the destruction, loss, modification,

unauthorized disclosure or access, accidentally or illegally, to data personal data transmitted, stored or otherwise processed ".

3.1. Failure to designate sub-processors.

For the purposes of compliance with the legislation on the protection of personal data, it is necessary to precisely identify the subjects who, for various reasons, can process personal data and clearly define their respective powers, in particular that of data controller and data processor and of the subjects operating under the direct responsibility of these (articles 4, points 7) and 8), 24, 28, 29 and 32, par. 4, of the Regulations and art. 2-quaterdecies of the Code).

During the investigations it emerged that the Company makes use of A1Tech S.r.l. (which carries out system management activities of the IT infrastructure of the service offered to AdB) and Agic Technology S.r.l. (which mainly carries out maintenance and specialist assistance on the application) and that "none of the aforementioned companies has been designated sub-manager of the processing that AiComply carries out on behalf of AdB" (see minutes XX, pp. 2 and 3) .

Moreover, as emerged during the investigation, AdB has not received communications or requests for authorization from the Company regarding the involvement of these subjects and their appointment as sub-processor (Article 28, paragraphs 2 and 4 , of the Regulation).

In this regard, the statements made by the Company regarding the fact that A1Tech S.r.l., in carrying out system management activities of the IT infrastructure, "does not process personal data of any kind (and even potentially has access to the data) cannot be considered acceptable. less in this case the obligation to appoint a sub-processor "and that" the substantive rationale of Article 28 RGPD [...], beyond the formal omission of the act of appointment as a sub-processor [di Agic Technology S.r.l.] can be considered prosecuted "in consideration of the guarantees presented by this subject to implement adequate technical and organizational measures (see note of XX), for the reasons set out below.

In the first place, it is believed that, given the definition of "processing of personal data" (Article 4, point 2) of the Regulation), also the system management of the IT infrastructure by A1Tech S.r.l. (which on the basis of the contractual documentation also includes the management and maintenance of the Company's IT systems) inevitably involves the processing of personal data referring to the users of the "WB Confidential" application, hosted on the Company's IT infrastructure, and to other interested parties whose personal data are present in the reports of illegal conduct acquired and managed with this application (see, on this point, also the provision no. 281 of 17 December 2020, web doc. no. 9525315).

A1Tech S.r.l., in fact, while not directly accessing the personal data processed within the application in question, carries out

"routine management and maintenance of the servers in the Rome office", in order to "keep the infrastructure operational (Hardware and Software) through activities that ensure continuity in the removal of malfunctions "," ensure timely improvement of functionality and presentations "," ensure the functional technical evolution of the hardware and software infrastructure "," provide support services to promptly resolve related problems to malfunctions and errors ", as well as" ensuring the periodic updating of the infrastructure, through the improvement of functionality, reliability and efficiency "(see Annex 5 to the minutes of the XXth, pp. 2 and 4). In carrying out the aforementioned activities, A1Tech S.r.l. has access to the Company's processing systems (including the one hosting the application in question) with a system administrator profile, ensuring certain levels of service in terms of availability and security of the systems themselves and making a series of tools to monitor the status of the IT infrastructure.

Based on the above elements, it must therefore be considered that, contrary to what the Company claims, the operations described above still give rise to the processing of personal data pursuant to art. 4, point 2), of the Regulation, also by A1Tech S.r.l. (see also the "Guidelines on the concepts of data controller and data controller in the RGPD", recently adopted by the European Committee for the protection of personal data and currently subject to public consultation).

Secondly, it should be noted that, consistent with the provisions of art. 28, par. 2, of the Regulations, in the deed of designation of the Company as data processor by AdB (see Annex 10 to the minutes of the operations carried out in XX, paragraph 10.2) it was expressly provided that, if the Company wished to resort to other persons responsible for carrying out certain activities related to the processing (in this case to A1Tech S.r.l. and Agic Technology S.r.l.), the same should have informed the data controller to allow him to express his possible opposition in this regard. This provision is, in fact, functional to ensure that the data controller always has full control of the treatments that are carried out on his behalf, being able, if necessary, to oppose both the very possibility of resorting to "other data processors", and the identification of these subjects as carried out by the "initial manager" (see Article 28, paragraphs 2 and 4, of the Regulation; with regard to the specific risks deriving from the failure to regulate the relationship, pursuant to Article 28 of the Regulation , with the subjects who process the data on behalf and in the interest of the data controller, provisions of 17 September 2020, nos. 160 and 161, web doc. n. 9461168 and 9461321; see also provision. XX, n. 49 , web doc. n. 9562852, as well as provision of 17 December 2020, n. 280, 281 and 282, web doc. n. 9524175, 9525315 and 9525337).

For these reasons, it must be concluded that the Company's use of the services offered by A1Tech S.r.l. and Agic Technology

S.r.l. - in the absence of a contract or other legal act governing the processing of personal data by the latter, and without the prior authorization of the data controller - occurred in violation of art. 28, para. 2 and 4, of the Regulation.

3.2. The security of the processing.

Preliminarily, it is noted that, 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) and that the same application did not provide for the encryption of personal data (identification data of the reporting party, information relating to the report as well as any attached documentation) stored in the relative database.

From the examination of the documentation produced in the last annex to the defense brief, it emerged, however, that "it was a precise economic and contractual choice of Aeroporti di Bologna to indicate to the Company to proceed with the development of the Application without adopting [... such] security measures ", as also confirmed by the technical-economic offer of" Supply and operational support for the implementation of an application for the centralized management of whistleblowing "of 31 August 2015 and the related supply contract of 14 September 2015 (see annex 2 and 3 to the note of the XX). For these reasons, the failure to use cryptographic tools for the transport and storage of data, in any case not in compliance with the provisions of art. 32 of the Regulations, cannot be considered attributable to the Company in practice.

During the investigation it also emerged that, although authorized for processing, two subjects operating under the authority of the Company and Agic Technology S.r.l. (Article 29 of the Regulation) used a single non-nominal user (called "agicwhistle \ spadmin"), with a system administrator profile, to access the "WB Confidential" application.

Taking into account the nature, object, context and purposes of the processing, which involves the acquisition and management of reports of unlawful conduct, which may contain personal data - also belonging to particular categories or relating to criminal convictions. and offenses (articles 9, par. 1, and 10 of the Regulation) - referring or referring to the reporting party, the person reported or third parties in any case involved in the reported facts, it is believed that the aforementioned methods of access to the "WB Confidential" application are adequate in terms of safety.

In this regard, the statements made by the Company regarding the fact that "no rule of the RGPD directly prohibits the sharing of users" and that "the sharing (only formal and nominative) of users as detailed above in concrete and the different activities (chronologically out of phase in time) carried out by the two system administrators in any case could not have entailed any "high and unjustified risk for the rights and freedoms of the data subjects" ". With regard to this last profile, the Company stated

that "concurrent accesses by the two directors" were not carried out and that "the sharing only lasted during the test and production phases of the Application" (see note of the XX). These defensive arguments cannot be considered relevant for the reasons set out below.

Noting that, even after the testing and production phases of the application, the password of the aforementioned user, having not been changed, was in the full availability of the person who had used it in these phases (see minutes of the 20th , p. 6, where it is stated that "the application does not require a mandatory change of the password of the account called" agicwhistle \ spadmin "after a certain period of time" and that "changing the relative password is not recommended as it could cause malfunctions of the application and interruption in the continuity of the service "), it is noted that the use of non-nominal users, by several subjects, prevents the actions performed in a computer system from being attributed to a specific subject, with prejudice, even for the data controller and data processor, who are in fact deprived of the possibility of controlling the work of subjects acting under their own authority.

Furthermore, when a non-nominal user with administrative privileges, such as the one in question, is used by several subjects, situations may arise in which there is no consistency between the authorization profiles assigned and the actual operational needs for the management of the systems. , thus making it possible for an unauthorized person to operate, in the absence of a specific will of the data controller or data processor, in the field of processing systems and services (under this specific profile, see provision of 4 April 2019, n.83, web doc. 9101974, and of January 14, 2021, n. 4, web doc. 9582744). More generally, although according to what was declared by the Company, the user in question would have been used in separate moments by the two system administrators, this circumstance does not exclude that the ascertained sharing of this user may have given or given rise to unauthorized access. to the data processed in the context of the "WB Confidential" application, in a way that does not comply with the principle of integrity and confidentiality and with the obligations regarding the security of processing.

Moreover, the use of "authentication credentials for the exclusive use of subjects operating under his authority or that of the data controller" in the previous regulatory regime was expressly provided for as a minimum security measure for which all data controllers were required to adopt (pursuant to the technical specification referred to in Annex B to the Code, in the text prior to the amendments referred to in Legislative Decree No. 101/2018), the violation of which also entailed the application of a criminal sanction (Article 169 of the previous Code).

In addition to the previously highlighted profiles, it emerged that the administrative management interface of the application in

question was accessible from the public network, with a weak IT authentication procedure (with a single factor) and without any automatic user blocking mechanism " agicwhistle \ spadmin ", in case of repeated failed authentication attempts. These methods of accessing the application entail a high and unjustified risk for the rights and freedoms of the data subjects, in consideration of the serious consequences, also in terms of possible discrimination or retaliatory behavior against the whistleblower, which could derive from any unauthorized access. authorized to the data contained therein.

For these reasons, considering that the Regulation has governed the obligations and specific responsibilities not only of the owner, but also of the data controller, also with regard to the security of the treatment (see articles 32 and 83, par. 4, of the Regulation), the methods of accessing the "WB Confidential" application, with the characteristics described above, do not comply with the provisions of art. 32 of the Regulation.

4. Conclusions.

In light of the aforementioned assessments, it is noted that the statements made by the data controller in the defensive writings for the veracity of which one may be called to answer pursuant to art. 168 of the Code although deserving of consideration and indicative of the full cooperation 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 violation committed, which - given the permanent nature of the alleged offenses - is still ongoing. Therefore, it is believed that 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 the absence of a contract or other legal act that governed the processing of personal data by two other companies , and without the prior authorization of the data controller, in violation of art. 28 of the Regulation, as well as in the absence of appropriate technical and organizational measures to ensure an adequate level of security for the risks presented by the processing, in violation of art. 32 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, par. 4, of the Regulation.

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

Considering that, to date, the Company has not proved that it has regulated the relationship with the companies A1Tech S.r.l. and Agic Technology S.r.l., having previously obtained the authorization of the data controller, nor has it provided evidence regarding the adoption of technical and organizational measures aimed at ensuring adequate methods of access to the "WB confidential" application by authorized personnel operating under the authority of the initial manager and other data processors, it is necessary to order the Company, pursuant to art. 58, par. 2, lett. d) of the Regulation, to conform the processing to the provisions on the protection of personal data (articles 28, paragraphs 2 and 4, and 32 of the Regulation), within thirty days of notification of this provision.

Pursuant to art. 58, par. 1, lett. a), of the Regulation and 157 of the Code, the Company must also communicate to this Authority, providing an adequately documented feedback, within thirty days from the notification of this provision, the initiatives undertaken to ensure compliance of the treatment with the Regulation.

6. 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).

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, for the protection of the interested party, a high degree of confidentiality with specific regard to the identity of the same and the circumstance that, with specific regard to the methods of accessing the application in question,

already in the previous regulatory framework, the sharing of authentication credentials between several authorized subjects was considered illegal (see spec. rule no. 4 of the technical specification referred to in Annex B to the Code, in the text prior to the amendments referred to in Legislative Decree no. 101/2018).

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.

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

Due to the aforementioned elements, assessed as a whole, also taking into account the phase of first application of the sanctioning provisions, pursuant to art. 22, paragraph 13, of the d. lgs. 10 August 2018, n. 101, it is believed to determine the amount of the pecuniary sanction, in the amount of € 20,000.00 (twenty thousand) for the violation of Articles 28 and 32 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 aiComply S.r.l. for the violation of articles 28 and 32 of the Regulations, within the terms set out in the motivation;

ORDER

to aiComply S.r.l., in the person of the pro-tempore legal representative, with registered office in Rome, via Castel Giubileo n. 62, C.F./P.IVA 10900531004, pursuant to art. 58, par. 2, lett. i), and 83, par. 4, of the Regulations, to pay the sum of 20,000.00 (twenty 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 aiComply S.r.l .:

a) to pay the sum of € 20,000.00 (twenty 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. d) of the Regulation, to conform the processing to the provisions on the protection of personal data (articles 28, paragraphs 2 and 4, and 32 of the Regulation), within thirty days of notification of this provision;

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 to ensure compliance of the treatment with the Regulation;

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

Ghiglia

THE SECRETARY GENERAL

Mattei