[doc. web n. 9767635]

Order injunction against Brav s.r.l. - March 24, 2022

Record of measures

n. 107 of 24 March 2022

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 / EC, "General Data Protection Regulation" (hereinafter the "Regulation");

GIVEN the legislative decree 30 June 2003, n. 196, "Code regarding the protection of personal data", as amended by Legislative Decree 10 August 2018, n. 101, containing provisions for the adaptation of national law to the Regulation (hereinafter the "Code");

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

GIVEN the documentation in the deeds;

HAVING REGARD to the observations of the Office made by the Secretary General pursuant to art. 15 of the Guarantor Regulation n. 1/2000 on the organization and operation of the office of the Guarantor for the protection of personal data, in www.gpdp.it, doc. web n. 1098801;

Rapporteur Dr. Agostino Ghiglia;

1. Introduction

Following a report received in the month of XX, as well as press news, the Authority learned that the platform used by the local police force of the Municipality of Genoa for the management of violations to the Highway Code, containing the personal data of citizens recipients of fines, was subject to unauthorized access by unauthorized parties.

In the same period, moreover, the aforementioned Municipality notified the Guarantor of a violation of personal data pursuant to art. 33 of the Regulation, from which it emerges that the abusive access would have been caused "by the careless behavior of some agents, who, violating the service provisions, would not have changed the first access password and disclosed the access URL".

2. Preliminary activity

In relation to the case, an investigation was initiated, during which it emerged that the Municipality of Genoa - data controller - entered into, on the 20th, a contract for the supply of "Scat" software licenses with Brav s.r.l. (hereinafter, the company), by regulating relations with it, pursuant to art. 28 of the Regulations, with a provision of the Mayor of the XX.

In response to a request for information from the Authority (note prot.n.XX of the XX) the Municipality of Genoa, with note of the XX (prot. Unauthorized access to the ScatWeb portal derives from the disclosure, by internal staff, of the access credentials (remained unchanged from those assigned to make the first access to the portal).

In particular, the Municipality stated that "at the time of the facts, the policies relating to the access credentials were as follows: at the first access, the Local Police operator was allowed to enter the ScatWeb platform by entering, both as a username and as a password, your serial number (badge), consisting of four digits. After the first access, the operator was obliged to change the access password with a new one consisting of at least four characters, as reiterated again to the operators with the last service order on the matter no. XX of the XX ".

In response to the request for information, the Municipality has attached, among other things, a note of the twentieth century, received by the company, which shows, on this point, that "with specific reference to the methods of accessing user profiles, the adoption of simplified credentials (first password equal to the Municipal Police user-agent serial number, reserved in any case only to agents with an "VERIFYER" profile) constituted a specific request formulated during the provision of training courses and subsequent telephone conversations , by the training managers of the Local Police (therefore, of the Owner himself) in order to simplify the distribution of the credentials to the user operators "and that" in the course of the relationships that have taken place to date, it was Brav himself who pointed out to the operational contacts of the Data Controller with whom he interacted for the management of the same portal, the opportunity to comply with the good practices in force on the matter for the the setting of passwords [… and having] provided the Data Controller with specific instructions for the subsequent password change that each operator could carry out independently ".

It also emerged that the company "on XX [...] requested, by e-mail sent to the heads of the Local Police, the adoption and activation by the same of more restrictive policies on access to the various user profiles, in in particular, expressly referring to the opportunity to adopt more complex password generation criteria ("8 characters of which 1 numeric, 1 alphanumeric, 1 special"), given that the ScatWeb portal allows this possibility to the Owner and its operators, in compliance to the indications of the AGID ", without receiving feedback.

On this point, however, the Municipality, with the aforementioned note of the XXth, represented the following:

- "The company managing the ScatWeb system should have imposed an IT obligation to change the password on first access, with the characteristics corresponding to the security obligations falling within the minimum security measures referred to in art. 32 GDPR. The BRAV Company had contractually assumed the burden of paying particular attention to the management of access credentials based on the principles of accountability and privacy by design. Failure to comply with this obligation therefore constitutes a breach of contract "and the company" claims to have received from the training managers of the Local Police, both during the training and in subsequent telephone contacts with them, the request to adopt simplified credentials (first password equal to the user-agent serial number, reserved only for agents with "VERIFYER" profile) in order to facilitate the distribution of the credentials to user operators ";

- "The Brav also claims to have highlighted to the Data Controller (more precisely to the operational representatives of the ScatWeb portal management) the opportunity to follow the good password change practices that each operator could carry out independently. As proof, he declares to have sent, on XX date, an e-mail to the heads of the Local Police, through his DPO, in which he requested the adoption and activation of more restrictive policies on access to the various user profiles and highlighted the opportunity to adopt more complex password generation criteria (“8 characters of which 1 numeric, 1 alphanumeric, 1 special”) in compliance with the AGID guidelines. The company declares that it has not received a reply to the aforementioned e-mail, despite the reminder of its DPO ";

- "According to Brav's conclusions, it is clear that, at the date of the event, the operational representatives of the management of the ScatWeb portal were perfectly aware of the type and level of complexity of the access credentials used by their operators-users and that the Owner of the processing had been appropriately advised by the same company regarding the advisability of adopting more complex access credentials than those that the Data Controller himself had actually requested to implement (clearly in derogation from any contractual indication). On the contrary, it should be noted that in the Local

Authorities the powers to manage contracts are - exclusively - of the executives, and that therefore a contractual provision can be modified only in the face of the written provision of the competent Executive. It is therefore evident that the verbal request of a subject, even if belonging to the organization of the Owner, but not endowed with powers of representation, is absolutely not suitable for modifying an essential characteristic of the service, especially to the extent that such request stands in clear contrast with the cardinal principles of accountability and privacy by design provided for by the European Regulation ".

Furthermore, during the preliminary investigation, it emerged that the platform in question was also available on the http protocol.

On this point, according to what was asserted by the Municipality of Genoa in the aforementioned note of the twentieth century, the company allegedly declared "that it had actually adopted this protocol but leaving the unsafe" http "protocol available and usable, in fact used by users who certainly could not have as a whole the necessary technical knowledge to prefer the secure protocol. Only after the notification via e-mail by the technical structures of the Data Controller, notification occurred on day XX, did the Brav company endeavor to automatically carry out the so-called "Redirect" from the "http" to "https" protocol for all incoming connections, making it impossible to use the insecure protocol ".

In this regard, with the note of the XXth, the company stated that "the https protocol has always been active with a regular valid certificate and therefore perfectly functioning and BRAV has provided the Owner with a specific indication to access the platform through this protocol" and that "for today, the undersigned company [.. has] already adopted all the technical adjustments aimed at correcting the criticalities you ascertained and detected […] and, in particular: - the modification of the url for access to the ScatWeb portal; - the reset of all access passwords; - the setting of the obligation to change the password at the first access with a password of high complexity. - automatic redirection of http calls on https protocol ".

In a subsequent response to a request for information from the Authority (prot.n.XX of the XX), the Municipality of Genoa provided further information (note of the XX), attaching a note of the XX of this company, which shows that "with reference to the issue of non-transmission of" system logs ", it should be noted that Brav maintains an active monitoring system of" system logs "in relation to all systems in which it carries out its activities, including the ScatWeb system, recognizing in this garrison a high form of cyber security. Files containing the "system logs" recorded by the server are attached. However, with specific reference to the tracking of IP addresses of accesses to the ScatWeb system, which are recorded by the webserver ("IIS log"), a few weeks before the occurrence of the data breach episode, the writer Brav has received warning messages from its server

monitoring system […], which showed that specific critical thresholds had been exceeded with the consequent risk of saturation of the main disk. Consequently, the technical intervention required the temporary and precautionary interruption of any source of further writing to the main disk, including the tracing of the "IIS logs", in order to avoid disk saturation and consequent serious damage, and this until the disk expansion operation is completed. Upon confirmation by the technician in charge of completing the aforementioned intervention, the "IIS log" tracking system was reactivated from the date of the 20th. As a result of the above, it is confirmed that: - due to the technical intervention described above, an IP address tracking report is not available to Brav for the required period from XX to XX ".

Therefore, with a note dated 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 Regulation, inviting the company 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 n. 689 of 11/24/1981).

With the aforementioned note, the Office found, first of all, that some unauthorized subjects had the opportunity to view the personal data of some interested parties by accessing the platform used by the Local Police of the Municipality of Genoa for the management of fines. . Furthermore, it emerged that the service in question was also available on http protocol, that is, through a network protocol that does not guarantee secure communication both in terms of confidentiality and integrity of the data exchanged and the authenticity of the website displayed. It is also established that, due to a technical intervention aimed at avoiding disk saturation, the company did not have the server logs, containing, among other things, the IP addresses of the accesses to the ScatWeb system, of the period in which it occurred. the violation of the personal data in question (XX - XX), in violation of articles 5, par. 1 letter f) and 32 of the Regulation.

With a note dated the XXth, the company presented its defense briefs, declaring that it “immediately committed itself to improving the services offered by adopting the following measures: - Brav has adopted rigorous procedures for the control of its systems; in particular, it has appointed two system administrators who, on a weekly basis, check the proper functioning of the systems and report them in a "periodic checks" report - A XX Brav has transferred all the services to the ARUBA Private Cloud (AGID qualified cloud) and from then every 6 months a Vulnerability assessment of the entire infrastructure is carried out. - In the month of XX Brav achieved the ISO27001 certification, including the guidelines ISO / IEC 27017, ISO / IEC 27018

".

With the subsequent note of 1XX, the company also declared “the shortcomings that have been attributed to our company relating to - IIS logs disabled - HTTP protocol active derive from human error and are absolutely not part of the practice. In fact, normally - the IIS logs are active - the automatic redirect of any HTTP call in HTTPS is applied. This is demonstrated by the fact that the countermeasures were applied very quickly, as they were usually active. To avoid future errors of this nature, an internal improvement process was immediately undertaken which led our company to achieve ISO 27001 certification with the further use of guidelines XX and XX on date XX. the AgID qualification and now the BRAV services are available on the homonymous marketplace. With the aforementioned certification, BRAV has adopted procedures such as: - Weekly surveillance of the state of the systems and establishment of appropriate documentation - Establishment of a security TEAM (System Admin and D.P.O.) ".

Finally, for the sake of completeness, it should be noted that, in response to a further request for information from the Authority (prot. XX of the XX) with the note of the XX (prot. XX) the Municipality of Genoa represented:

“The employees of the Local Police Corps Management process personal data in compliance with the security measures provided and the instructions given by the Commander. The Management has formalized with the internal Circular [...] the methods of processing personal data for the "persons in charge of processing";

"For the correct use of the application for the management of the sanctioning system (Scat), the Management has provided, before its implementation, to train the staff through specific courses in the presence, providing technical elements on the use of the program and raising awareness of the staff on the correct treatment of the personal data collected ";

"In the Training Plan of the Municipality of Genoa, three-year period 2021-2023, [...] there is a continuous training program on the protection of personal data of a transversal nature for all employees, for example, on issues such as security measures ICT, the principles of the GDPR, the protection of personal data in the public context, etc. together with other relevant aspects, such as eg. the digital transition ";

"The Body is continuing to review internal procedures regarding the protection of personal data, through a more substantial and less formal approach than the fulfillment of the Privacy Code. In this regard, the Entity has adopted a Regulation on the protection of personal data and privacy, [...] in order to make the organizational structure more consistent with the principles of Regulation (EU) 2016/679 by operating, among others, a qualification of the role of the executives who carry out the

processing in relation to the databases of the areas of competence, with a view to a strong link between the management of human and financial resources and the management of personal data ";

"As a demonstration of the attention of the Entity towards the protection of personal data, it should be considered that already in the twentieth century, and therefore before the data breach, the data controller with a note from the Personnel Department [...] had made the correct management of passwords, raising awareness of their inappropriate use "increases the risk of unauthorized access, which can trigger problems or threats to the security of the Entity's data processing";

"Contravening a specific service order no. [...] on the occasion of the data breach, all the security measures imposed by the Body were disregarded ";

"With regard to the internal technical measures taken, also in order to raise the staff's awareness of compliance with the legislation on the protection of personal data and avoid the repetition of similar violations in the future, it is represented that at the time of knowledge of the criticality on the date XX, the Offenses Department promptly contacted the BRAV company so that, in its capacity as manager of the Scat system, it would block all accesses where the password had never been changed, as well as subsequently check the critical issues. From the date of the twentieth [... the company] has increased the password security level, imposing the computer obligation to change the password at the first access with an access key of high complexity compared to the previous one (serial number), consequently, if the password is not replaced access is not allowed, moreover, the password must be changed every three months and has the following characteristics: extension between 8 and 12 characters, at least one uppercase, at least one lowercase, at least one number, at least a special non-alphanumeric character. With the imposition of the password change after the first access and with continuous training, behaviors oriented towards greater prudence on processing activities can be observed, also due to an increased sense of awareness on the risks involved in the processing of personal data ";

"The Entity is in the process of adopting new guidelines on the correct use of IT tools provided to employees (eg. Laptops, tablets, mobile phones, smart phones)";

"The Authority has also taken steps to intensify control over the supplier's work. In particular, a six-monthly vulnerability assessment of the entire infrastructure was required, which was performed during the month of XX [...]. A penetration test was also performed on the server hosting the procedure ".

3. Outcome of the preliminary investigation

According to the rules on the protection of personal data, public subjects can process data only if necessary "to fulfill a legal obligation to which the data controller is subject" or "for the execution of a task of public or related interest the exercise of public authority vested in the data controller "(Article 6, paragraph 1, letter c) and e) of the Regulation). In this context, the management of administrative violations and violations of the Highway Code is one of the institutional activities entrusted to local authorities.

As emerged during the investigation, the processing of the data in question is carried out by the company on behalf of the Municipality of Genoa. Pursuant to art. 28 of the Regulation, in fact, the owner can also entrust processing to third parties who present sufficient guarantees on the implementation of technical and organizational measures suitable to ensure that the processing complies with the regulations on the protection of personal data (" treatment").

Even in the presence of a condition of lawfulness, in any case, the processing of personal data must take place in compliance with the principles of data protection, including that of "integrity and confidentiality" under which the data must be " processed in such a way as to guarantee adequate security of personal data, including the protection, by means of adequate technical and organizational measures, from unauthorized or unlawful processing and from accidental loss, destruction or damage "(Article 5, par. 1, lett. and f) of the Regulation).

Art. 32 of the Regulation places both the owner and the manager in charge - taking into account the state of the art and the implementation costs, as well as the nature, object, context and purposes of the processing, as well as the risk - the adoption adequate technical and organizational measures to ensure a level of safety appropriate to the risk, which include, among others, where appropriate "a procedure for regularly testing, verifying and evaluating the effectiveness of technical and organizational measures in order to guarantee safety of the treatment ".

As previously clarified by the Guarantor, certain obligations are also placed directly on the manager himself who, also based on the specific technical skills, must collaborate, also by showing a proactive autonomy, in the adoption of adequate measures and in the systematic verification of effectiveness of the same, especially if it provides services to a plurality of data controllers involving a large number of data subjects, as in the case in question (see provisions no.48 of 11 February 2021, web doc. 9562831 and n. 293 of 22 July 2021, web doc. N. 9698597).

The company, precisely because of its experience in the sector, was required to constantly check the effectiveness of the measures placed in charge of the platform provided to the Local Police of the Municipality of Genoa for the management of

fines, as well as clearly also regulated in the trade union provision of appointment, as data processor, of the XX.

On the other hand, it is ascertained that some unauthorized subjects have had the opportunity to access the aforementioned platform. Although, in summary, it emerged that this access took place due to a leak of confidential information (credentials) by internal staff of the local police force of the Municipality of Genoa, the company should in any case have adopted technical and organizational measures aimed at ensure that the passwords of authorized parties complied with quality criteria and were obligatorily changed on first use.

Furthermore, it emerged that the service in question was also available on http protocol, that is, through a network protocol that does not guarantee secure communication both in terms of confidentiality and integrity of the data exchanged and the authenticity of the website displayed. It is also ascertained that, due to human error, the company did not have the server logs containing, among other things, the IP addresses of the accesses to the ScatWeb system, of the period in which the violation of the personal data in question took place (XX - XX).

Therefore, it is ascertained that the company has not adopted technical and organizational measures suitable to guarantee a level of security adequate to the risks presented by the processing, in violation of Articles 5 par. 1 letter f), and 32 of the Regulation.

For the sake of completeness, it should be noted that, based on the elements collected, the conditions for adopting a prescriptive or inhibitory provision by the College against the Municipality of Genoa are not recognized (see Article 11 of Regulation no. 1/2019 of 4 April 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).

This is because it was taken into account that in the act of appointment as a data processor pursuant to art. 28 of the Regulation, the Municipality of Genoa has explicitly provided for, among other things, the obligation for the company, due to its technical experience in the sector, to implement adequate technical and organizational measures to guarantee an adequate level of safety. risk including a procedure to test, verify and regularly evaluate the effectiveness of technical and organizational measures in order to guarantee the security of the processing.

Finally, it was acknowledged that the Municipality of Genoa has taken action not only to restore the security measures appropriate to the risks presented by the treatment, but also to ensure awareness of internal staff with guidelines, internal circulars, and permanent training regarding the protection of personal data.

4. Conclusions

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

From the checks carried out on the basis of the elements acquired, also through the documentation sent, as well as from the subsequent assessments, the non-compliance of the treatments carried out by the company on behalf and in the interest of the Municipality of Genoa concerning the supply of the portal used by the local police body for the management of fines.

The violation of personal data, object of the investigation, took place in full force of the provisions of the Regulation and the Code, as amended by Legislative Decree No. 101/2018, and therefore, in order to determine the regulatory framework applicable under the time profile (art. 1, paragraph 2, of the l. 24 November 1981, n. 689), these constitute the provisions in force at the time of the aforementioned violation.

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 technical and organizational measures suitable to guarantee a permanent level of security and adequate to the risk presented by the processing. , in violation of art. 5 par. 1 letter f), and 32 of the Regulation.

The violation of the aforementioned provisions makes the administrative sanction applicable pursuant to art. 58, par. 2, lett. i), and 83, para. 4 and 5, of the same Regulation, as also referred to by art. 166, paragraph 2, of the Code.

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

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

In this regard, taking into account art. 83, par. 3, of the 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, it was considered that the processing of personal data collected through the portal used by the local police force of the Municipality of Genoa for the management of fines, probably starting from the month of XX (period in which the collaboration with the Municipality of Genoa), and up to the 20th, took place in the absence of technical and organizational measures suitable to guarantee a level of security adequate to the risks presented by the processing.

This violation was brought to the attention of the Authority through a report and notification of the violation of personal data pursuant to art. 33 of the Regulation.

On the other hand, it was considered that no other complaints or reports were received that could lead one to believe that the aforementioned violation may have involved a significant number of interested parties. From what emerged, in fact, from the investigation (note from the Municipality of Genoa of the 20th century), "with regard to the data breach in question, it can be assumed that accesses were made only for demonstration purposes by the same journalist, without the will or the need to acquire the data entered in the system. In fact, access made on day XX with the serial number [...] referred to in the article and therefore presumably used by the journalist), would seem to have consulted only the data of the vehicle [...] owned by the same journalist [...] It can be stated with reasonable assurance that no other access has been made by the readers of the article, as on the day of publication of the same (XX) the profiles had already been disabled on XX for precautionary reasons (as indicated in letter h of this note) to following the aforementioned report ".

It was also taken into account that the company took immediate action to remedy the violation and mitigate its possible negative effects, collaborating with the data controller.

In any case, the non-malicious behavior of the violation is highlighted.

Finally, there are no previous violations of the Regulations committed by the company.

Due to the aforementioned elements, assessed as a whole, it is deemed necessary to determine pursuant to art. 83, par. 2 and 3, of the Regulations, the amount of the pecuniary sanction, provided for by art. 83, par. 5, lett. a) of the Regulations, to the extent of € 10,000 (ten thousand) for the violation of Articles 5, par. 1, lett. f) and 32 of the Regulation as a pecuniary

administrative sanction deemed effective, proportionate and dissuasive pursuant to art. 83, par. 1, of the same Regulation.

Taking into account the failure to adopt adequate technical security measures, it is believed that the ancillary sanction of the publication on the website of the Guarantor of this provision, provided for by art. 166, paragraph 7 of the Code and art. 16 of the Guarantor Regulation n. 1/2019.

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

WHEREAS, THE GUARANTOR

declares the conduct held by Brav s.r.l. unlawful, for the violation of articles 5, par. 1, lett. f) and 32 of the Regulations, within the terms set out in the motivation,

ORDER

a Brav s.r.l., in the person of the pro-tempore legal representative, with registered office in Vignola (MO), Via del Portello n. 4 / B, 41058, - Tax Code 02818030369 - to pay the sum of € 10,000 (ten thousand) as a pecuniary administrative sanction for the violations mentioned 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 30 days, an amount equal to half of the sanction imposed;

INJUNCES

to Brav s.r.l., to pay the sum of € 10,000 (ten 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 and art. 16, paragraph 1, of the Guarantor Regulation n. 1/2019;

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

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

Rome, March 24, 2022

PRESIDENT

Stanzione

THE RAPPORTEUR

Ghiglia

THE SECRETARY GENERAL

Mattei