[doc. web no. 9889644]

Provision of April 13, 2023

Register of measures

no. 121 of 13 April 2023

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

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

HAVING REGARD TO Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, concerning the protection of natural persons with regard to the processing of personal data, as well as the free movement of such data and which repeals Directive 95/46/ CE, “General Data Protection Regulation” (hereinafter, “Regulation”);

HAVING REGARD TO Legislative Decree 30 June 2003, n. 196 containing the "Code regarding the protection of personal data, containing provisions for the adaptation of the national legal 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 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”);

CONSIDERING the Regulation n. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor for the protection of personal data, approved with resolution no. 98 of 4/4/2019, published in the Official Gazette no. 106 of 8/5/2019 and in www.gpdp.it, doc. web no. 9107633 (hereinafter "Regulation of the Guarantor n. 1/2019");

HAVING REGARD to the documentation in the deeds;

HAVING REGARD TO the observations made by the general secretary pursuant to art. 15 of the Regulation of the Guarantor n. 1/2000 on the organization and functioning of the Guarantor's office for the protection of personal data, doc. web no. 1098801;

SPEAKER the lawyer Guido Scorza;

WHEREAS

1. The complaint.

With a complaint presented to the Authority, the lawyer XX represented an alleged violation of the regulations on the protection

of personal data concerning the registration procedure on the web portal "https://..." through which it is possible to access the services relating to the free legal aid activated by the Ancona Bar Association (hereinafter "Order" or "Advice"). In particular, the complainant complained that, in order to be able to submit an "application for admission to free legal aid" for its clients, it is necessary to use the aforementioned portal "as the only way to be able to forward the application" and that "the profile activation procedure - in addition to various data - expressly asks for the PEC BOX of the professional and THE PASSWORD TO ACCESS THE CERTIFIED ELECTRONIC MAIL BOX".

From the preliminary investigation carried out by the Office on the 20th date, it emerged that, at the web address https://..., it is possible to access the services relating to legal aid activated by the Order or make a new registration. In particular, the registration form requires, among other things, the insertion of the following information: registration data (name, surname, tax code, jurisdiction, address of the law firm); CD. "PEC parameters" (PEC address, PEC manager, PEC user and PEC password); access parameters (tax code and password); declarations about enrollment in the "list of lawyers for legal aid" and having read the "privacy information (information available on the website of the lawyers' association)".

2. The preliminary investigation.

With a note of the XX (prot. n. XX) responding to the request for information formulated by this Authority, the Order declared, in particular, that:

“the processing of data relating to the activities carried out on the aforementioned portal falls within the cases envisaged by art. 6 paras. 1 and 3 of the Regulation as necessary for the execution of a task of public interest or connected to the exercise of public powers with which the data controller is invested. The portal has been active since July of the XX”;

"the regulatory source that legitimizes the application of the aforementioned provisions, according to the provisions of the aforementioned par. 3 of the Regulation as well as by art. 2 ter of the Code, [...] consists of Presidential Decree 115/02" pursuant to which "the application for admission to legal aid containing all the information useful for assessing the non-manifest groundlessness of the application as well as those relating to the exceeding the established income limits, it is compulsorily presented to the Council of the Bar Association having territorial jurisdiction in accordance with the provisions of art. 124 of the aforementioned consolidated text”;

"[...] the use of the electronic platform in the manner envisaged by this is not mandatory and it is not the only way to present the application as the same can be filed "on paper" or sent by registered letter in traditional mode”;

"The dedicated platform allows you to process the applications and bring them to resolution in a very short time to facilitate the applicant who is entitled to free legal aid [...] this also in consideration of the fact that most of the applications are based on reasons of hardship social and economic, [...] which deserve to be examined as quickly as possible";

"To guarantee all the actors involved in this procedure, the platform uses certified e-mail which among its functions guarantees the date of presentation, makes clear the origin and guarantees the authenticity of the receipts. In practice, the request for PEC parameters is necessary as the applicant's defense attorney fills out the application on the platform which then forwards the application to the Bar Association, whose resolution is communicated to the same address. The computer system therefore accesses the PEC of the defender of the instant in order to use this mailbox only and exclusively for forwarding the application for admission to the benefit. The data required for registration therefore have the purpose of being able to examine all the requests presented quickly and correctly and make sure that the presentation is made by Lawyers registered on the appropriate lists";

"In full compliance with the GDPR 679/2016 and in particular with the art. 6 par 1 paragraph a) and e) the processing of data collected during registration is carried out by the data controller both for express consent and for the execution of a task of public interest".

With a subsequent note of the XX (prot. n. XX), the Board has, in particular, clarified that:

with reference to the publication on the website of a notice which provides for the mandatory use of the special portal for the filing of all applications for legal aid at the expense of the State, "The need to indicate a date on the Order's website, starting from which the requests had to be formulated through the use of the electronic platform arose from the large number of paper requests that had to be processed by the staff of the Secretariat. By also indicating the option of paper filing on the Order's website, almost all of the requests would have been received, at the secretariat, in paper form, with a considerable increase in work for the same";

"In designing the software for free legal aid, various methods of presenting the applications were evaluated and it was agreed to proceed with the transmission electronically via PEC and digital signature, also having regard to art. 65 of Legislative Decree 7 March 2005, n. 82, a solution that guarantees the authenticity of the document and the certainty of the date of presentation of the application, […] a fundamental element for compliance with the deadlines for processing the requests";

"As regards the authentication credentials [(username and password) for accessing the PEC mailboxes of the lawyers] these

are requested during registration with the aim of verifying whether the entered parameters allow sending at the time of presentation of the application and are in no way saved on the servers given that the "free legal aid" portal received the technical cookie from the user's browser in order to be able to send the digitally signed application via PEC to a box dedicated to receiving it";

“The password was encrypted with the AES256 algorithm and stored in a technical cookie in the user's browser. When the application is sent via PEC, the user's browser sends the technical cookie containing the encrypted code, [...] the algorithm used is AES256 which uses a specific part of the tax code and a fixed part known only by the server, the system decrypts it and allows the user to send the request, after this operation there is no trace of the password”;

“Having regard to the provisions of art. 122 of the code with reference to technical cookies, it was decided to facilitate the use of the platform by the user who requested it while maintaining a high standard of security”;

"technical cookies are those used for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary for the provider of an information society service explicitly requested by the subscriber or user to provide such service";

"We do not have any PEC mailbox authentication credentials saved on our servers".

The company Servicematica S.r.l., on the 20th date, specified, among other things, that "The system manages the password of the user's PEC box by means of a technical cookie released on the user's PC and encrypted with the AES256 algorithm and with a key composed of a part of the tax code. Basically, in order to use the user's PEC mailbox and send the application, the system must use the technical cookie encrypted with AES256 provided by the user, decrypt it with the encryption key "part of the tax code", send the application, eliminating then the password used. Each time the password must be used, it is recreated through the system described above. If the technical cookie is not found, the system will ask the user for the password again”.

Subsequently, the Council, with note dated XX, represented the following:

"As regards the authentication credentials [for accessing the PEC mailboxes of the lawyers] these are requested during registration with the aim of verifying whether the entered parameters allow sending when the application is presented and are not in no way saved on the servers given that the "free patronage" portal received the technical cookie from the user's browser in order to be able to send the digitally signed application via PEC to a box dedicated to receiving it";

"The system narrated above and referred to in the abstract of the previous communications has not even been used for years

because, given the various browser updates regarding security which sometimes did not make the above harmonious, it was opted to request the password of the pec each time NOT registering it anywhere in previous communications", specifying that, when registering on the portal, "the pec password is required only to verify the correctness of the data entered (by sending a test pec) ";

"In practice, once registration has been completed to access the portal, the tax code and a password that the user generated during registration is requested, where there is the specific reference to the privacy information whose link correctly refers to the information prepared by Servicematica, having completed the application to be able to send it by certified mail, a message appears requesting the insertion of the PEC password", also attaching a copy of this information.

Based on the elements acquired, the Office notified the Order, as data controller, pursuant to art. 166, paragraph 5, of the Code, the initiation of the procedure for the adoption of the provisions pursuant to art. 58, par. 2, of the Regulation, as the processing of personal data of lawyers (about 1,078 interested parties), carried out within the "https://..." portal in order to be able to submit applications for admission to free legal aid, activated by the The order was made in violation of articles 5, par. 1, lit. a), and 2; 13 and 25 of the Regulation and the processing of the authentication credentials of the PEC boxes of the lawyers (username and password), was carried out in violation of the articles 5, par. 1, lit. a) and f), 6 and 25 of the Regulation as well as of the art. 122 of the Code. Therefore the aforesaid owner was invited to produce written defenses 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 Law No. 689 dated 11/24/1981).

The Order sent its defense briefs representing, in particular, that:

"On the twentieth date, the previous Board in office entrusted Servicematica s.r.l. [...] the service relating to the creation of a portal for the telematic management of legal aid at the expense of the state [...]: it should be noted that the current Council took office in April XX";

"The Board had chosen to entrust this service to Servicematica s.r.l., as a subject in possession of both technical-professional requisites deemed adequate, both high certification standards, and documented experience in other Professional Orders. The service entrusted provided for the complete telematic management of all the phases relating to the applications for admission, including their logging. On the same date, Servicematica s.r.l. was appointed external data processing manager pursuant to art. 28 of the GDPR";

"On XX [...] the Order received a note from the manager in which [...] it was highlighted that the acquisition of the data [(authentication credentials for access to the PEC box)] was necessary "to guarantee the shipment of the application via PEC, so as to ensure the date of submission and receipt of the applications, any requests for integration of documents and resolutions and guarantee the origin and integrity". From a technical point of view, the manager ensured the absolute security of data processing as the service was accessible via the https protocol and subject to encryption according to advanced encryption algorithms, in addition to other guarantees of vigilance and security, all activities carried out by subject in possession of ISO 27017, 27018, 27001 and 27003 certifications";

with reference to the notice "which informed users that all applications for admission should have been filed exclusively electronically", "it should be noted that the same is a typo that was published on the Order's website following the activation of the portal by part of the previous council meeting and that in reality what is described therein was not considered binding by the present Council currently in office: as proof of this, in fact, it is declared that from the year XX to today they have been delivered in paper form and / or by PEC directly to the writer of the Order and therefore NOT through the portal, a total no. 125 instances […]. Furthermore, having deemed it necessary to agree with what was stated by the DPO regarding the methods for removing this notice, it should be noted that the same was effectively canceled from the site as a result of the resolution adopted by the Board";

“On the 20th date, the Order provided the requested reply, also attaching the privacy information prepared independently by the manager Servicematica s.r.l. and communicated by him […]. With respect to this information text attached to the communication, it is important to highlight that it is not the one relating to the service subject to verification by the Guarantor, but the text of the information relating to the treatment, by Servicematica s.r.l., of the data of its customers to title of independent Data Controller, for its own purposes, usually provided by Servicematica itself when accessing its website. It therefore has no relevance, for the purposes of the ongoing proceedings, as it is a document unrelated to the services and treatments subject to verification by the Guarantor";

"Having taken into account the considerations referred to in the notification" of the violation pursuant to art. 166, paragraph 5, of the Code "the Order immediately arranged for the precautionary suspension of the portal, inviting the manager to provide prompt response to the aforementioned [...]. As can be seen from the Order's website, following the suspension, a system was activated which provides for the download of the fillable pdf form which is then sent by PEC to the Order: substantially, to date

the compilation and transmission is not active telematics of applications";

"on XX [...] the Order invited Servicematica to produce a detailed report on the point highlighted in the notice received from the GPDP". "This request was necessary precisely in consideration of the notification and taking into account the fact that the Order - in which there are no professionals with specific IT training - had deemed it correct to rely on a person professionally suitable for the creation of an IT structure that would allow the electronic management of requests for admission to legal aid at the expense of the State. Given the results of the procedure proposed by the intestate Guarantor, it is at this point legitimate for the undersigned Order to doubt the validity of the arguments presented by the manager, on which the issues of the present proceeding largely depend. [...] the design of the portal including the provision of the request for access credentials to the PEC of the requesting defender derives from a specific design indication of Servicematica which represented to the undersigned Order the absolute need to obtain the aforementioned data as it is equally necessary to a correct management of the requests and also highlighted how the aforementioned portal had already been activated with the same precautions and the same technical methods for other forensic orders.";

"Despite this, deeming the punctual response to what is indicated in the notification to be indeed a duty, this Order has proceeded to commission the manager to completely redesign the portal in order to activate a system that DOES NOT require the insertion of the PEC credentials at the time of registration and therefore uses other systems to guarantee the effectiveness and safety necessary for the correct performance of the task that the law entrusts to the Bar in relation to the admission of applicants to legal aid at the expense of the State.";

"While waiting to be able to view and evaluate the new portal project, the Order has proceeded [...] to order the suspension of access and has proceeded to activate a "manual" system through which the Lawyer who intends to submit a application for admission to legal aid proceeds with the compilation of a form in .pdf format which is then sent to the Order by certified e-mail and entered into the system by personnel of the Order to then be processed by the Councilors in charge of the preliminary verification of the applications which follows the resolution of provisional admission to the requested benefit [...]. This procedure, although more laborious, avoids the involvement of third parties, with a view to the so-called privacy by default";

"As regards disputes regarding the content of the privacy policy, the following must be stated. The notification underlines [...] that the information necessary to ensure correct and transparent treatment would not have been provided to the interested parties and it is underlined that despite the aforementioned registration form found upon accessing the portal "required to have

read the privacy information (information available on the lawyers' association website) there was no link to this information on this page". Indeed, in the original structure of the portal, it was indicated that the information was published directly on the Order's website, but the presence of a hypertext link to this page has not been established. The aforesaid information, in relation to which users were required to proceed with acknowledgment, has in fact always been contained, and can always be consulted, at the web address https://.../. Following the findings of the Guarantor, therefore, steps were taken to prepare a hypertext link positioned for accessing the portal and within the procedure for registering a new user for the services, which refers directly to the privacy information. In this regard, Servicematica, in its capacity as external data processor, was asked to make any necessary changes in this regard, together with any further specific arguments";

with reference to "the provisions of art. 83 paragraph 2 of the regulation. 1. As for paragraph a) it can only be recalled that the purpose of the processing in question is functional to the performance of a service aimed at automated access to legal aid and therefore in connection with a judicial proceeding to be activated or even already activated in civil proceedings so that the same was deemed necessary for the execution of a task of public interest or connected to the exercise of public powers vested in the data controller in accordance with the provisions of art. 6 of the Regulations, without prejudice to the foregoing regarding the fact that the necessity under a technical profile of this treatment has been represented to the undersigned Order by the professional person in charge of providing for the creation of the portal. In terms of seriousness, we believe we can say that this element is hoped to be considered of a rather modest level, taking into account that the aforementioned credentials have not been subject to any dissemination and no damage has been caused by the aforementioned treatment. In this regard, reference is made to the infra deductions regarding the small number of users for the service, compared to the requests for accreditation received, in the years for which it is being investigated, by analogical paper method. It is also considered important to highlight that the treatment was not carried out in the context of a commercial activity or in any case in the context of a lucrative activity, so that the Bar Association did not receive any advantage or any economic benefit from the aforementioned treatment. As regards the duration, it is believed that it can be stated that the period concerned is between the month of July XX and May XX, and has not continued since then";

"As for paragraph b) In the hope that the Order will recognize good faith and correctness with the consequent exclusion of any subjective element, having in any case to ascribe the matter to the scope of willful or negligent conduct, it is believed that the same may be qualified in terms of fault due to the fact that the Order was induced to proceed with the treatment by virtue of

technical indications according to which the treatment was to be considered necessary and therefore a conditio sine qua non as regards the use of the portal for the 'insertion of requests for admission to legal aid at the expense of the State [...].";

“As regards paragraph d) please refer to the reports sent by Servicematica which represent the very high level of security of the IT structure concerning the processing of the data. As proof of the effectiveness of the established security level, it should be noted that as of the date of the portal's activation in the year XX, there has been no loss or illicit dissemination of the data [...]";

"As regards paragraph f) it is deemed possible to state that the Order promptly responded to the Authority's request during the investigation, proceeded to request the appropriate clarifications from the technical body in charge of building the portal and managing of the same as well as to order the immediate suspension of the same following the outcome of the Authority's considerations regarding the reasons of a technical nature that were presented in the aforementioned course. It can therefore be considered that the Order has offered the highest degree of cooperation".

During the hearing held on the 20th date, the Order represented that:

- "lawyers have always had the possibility, both before and after the intervention of the Authority, to submit applications for admission to free legal aid at the expense of the State both in paper and electronic form via PEC, as well as with the portal object of the this proceeding";
- "the Order decided to entrust the company Servicematica S.r.l. the creation and management of the portal in question as this subject was in possession of adequate technical-professional requirements and provided the same service to other Bar Associations";
- "the company Servicematica S.r.l., in its discussions with the Order, has always maintained that the procedure for presenting the requests adopted in the context of the service in question was adequate and represented the only way to provide the service";
- "the Order became aware of the matter directly from the Authority, having not received any report in this regard which would have allowed the problem to be managed and resolved more quickly with a view to accountability";
- "the Order promptly proceeded to suspend the service in question following receipt of the act of initiation of this proceeding";
- "the Order and the company Servicematica S.r.l. have not received any request for compensation for damages from the interested parties and have no evidence of any violation of the personal data processed in the context of the service in

question".

3. Outcome of the preliminary investigation.

3.1 Applicable legislation.

Pursuant to the European Regulation, which became applicable from 25 May 2018, "personal data" means "any information relating to an identified or identifiable natural person ("data subject")". Furthermore, "an identifiable natural person is one who can be identified, directly or indirectly, with particular reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more characteristic elements of his physical, physiological, genetic, psychic, economic, cultural or social identity" (art. 4, point 1), of the Regulation).

Public subjects, such as professional associations, may process personal data if "the processing is necessary for the execution of a task of public interest or connected to the exercise of public powers" (art. 6, par. 1, lett. e), and 3, lett. b), of the Regulation and art. 2-ter of Legislative Decree no. 196 of 30 June 2003, Code regarding the protection of personal data - hereinafter, the "Code"), previously providing the interested parties with information on the processing of personal data (articles 12, 13 and 14 of the Regulation).

More generally, European legislation provides that "Member States may maintain or introduce more specific provisions to adapt the application of the rules of this regulation with regard to treatment, in accordance with paragraph 1, letters c) and e), determining with greater precision specific requirements for processing and other measures aimed at guaranteeing lawful and correct processing [...]" (Article 6, paragraph 2, of the Regulation).

The data controller is, in any case, required to respect the principles of "lawfulness, correctness and transparency" and "integrity and confidentiality" according to which personal data must be processed "in a lawful, correct and transparent manner towards of the interested party" and "in such a way as to guarantee adequate security of personal data", as well as to demonstrate compliance with the aforementioned principles in compliance with the principle of "accountability" (Article 5, paragraph 1, letters a) and f) , and 2, of the Regulation).

The data controller, in accordance with the principles of "data protection by design" and "data protection by default", must also put in place "appropriate technical and organizational measures [...] aimed at effectively implementing the data protection principles, such as minimisation, and to integrate the necessary guarantees in the processing in order to meet the requirements of the [...] regulation and protect the rights of data subjects" as well as "adequate technical and organizational

measures to ensure that they are processed, by default by default, only the personal data necessary for each specific purpose of the processing" (Article 25, paragraphs 1 and 2, of the Regulation).

Finally, it should be noted that "the filing of information in the terminal device of a contractor or a user or access to information already archived are permitted only on condition that the interested party has given his consent after being informed in a simplified manner . This does not prohibit any technical archiving or access to information already archived if aimed solely at carrying out the transmission of a communication over an electronic communications network, or to the extent strictly necessary for the provider of an information society service explicitly requested by the contracting party or by the user to provide this service" (Article 122 of the Code).

3.2 The lawfulness and security of the processing.

As can be seen from the deeds and declarations made by the data controller as well as from the verification carried out on the basis of the elements acquired following the preliminary investigation and the subsequent evaluations of this Department, the Order has carried out the processing of the authentication credentials of the PEC boxes of lawyers in the absence of an appropriate legal basis.

Indeed, from the documentation in the deeds it appears that the Bar, starting "from the month of July of the twentieth century", made available a portal ("https://..."), through which the lawyers were required to enter and manage applications for free legal aid.

In particular, the registration form at the address "https://..." as well as information relating to the registration data (name, surname, tax code, place of residence, address of the law firm), the access parameters (tax code and password) and to the declarations regarding the registration in the "list of lawyers for legal aid" - requested the insertion of the so-called "PEC parameters" ("PEC address", "PEC manager", "PEC user" and "PEC password").

In this regard, the Council declared that the reasons that would have made the adoption of the aforementioned portal necessary would be linked to the need to "work the requests and bring them to resolution in a very short time to facilitate the applicant who is entitled to free legal aid [...] this also in consideration of the fact that most of the requests are based on reasons of social and economic hardship, [...] which deserve to be examined in the shortest possible time" and that the legal basis of the treatment would be constituted by the Presidential Decree no. 115/2002. It was also represented that "the processing of data collected during registration [... was] carried out [...] both for express consent and for the performance of a

task in the public interest".

At first, the Board stated that the passwords for accessing the PEC mailboxes of the lawyers, "requested during registration with the aim of verifying whether the entered parameters allow for sending at the time of presentation of the application", even if they do not were "in no way saved on the servers", were "encrypted [e] with the AES256 algorithm and memorized [e] inside a technical cookie in the user's browser".

Subsequently, on the 20th date, the Council highlighted that the aforesaid methods of processing the authentication credentials of lawyers' PEC mailboxes have not been used "for years because, given the various browser updates regarding security which sometimes did not make the above, you opted to request the pec password for each sending" specifying that, when registering on the portal, "the pec password is only required to verify the correctness of the data entered (by sending a test pec) ".

With regard to the above, the following is noted.

Preliminarily it should be noted that the processing of personal data consists of "any operation or set of operations, performed with or without the aid of automated processes and applied to personal data or sets of personal data, such as the collection, registration, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, diffusion or any other form of making available, comparison or interconnection, limitation , cancellation or destruction" (art. 4, point 2), of the Regulation).

Based on the elements listed above, it must be considered that the operations described give rise to the processing of personal data by the Order, subject to the application of the regulatory framework on the protection of personal data.

In the case in question, in fact, it emerges from the declarations that the Order, even though it has not kept any authentication credentials of the PEC boxes of the lawyers (username and password) on the IT systems managed by Servicematica S.r.l. on behalf of the Order:

- at least up to the date of the XX, has carried out processing of the aforementioned personal data, both at the time of registration of a user to the portal in question (when the password, unencrypted, was collected, encrypted and memorized within a alleged "technical cookie"), and when submitting an application for admission to legal aid (moment in which the password, stored in encrypted form within the aforementioned "technical cookie", was collected, decrypted and used by the portal to send, on behalf of the lawyer, the PEC message containing the application);

- also following the modification of the functioning of the portal in question, has carried out the processing of the aforementioned authentication credentials of the PEC boxes both at the time of user registration ("with the aim of verifying whether the entered parameters allow sending in the time of presentation of the application"), and at the time of presentation of each application for legal aid at the expense of the State (for sending, on behalf of the lawyer, the PEC message containing the application).

Having said this, it should be noted that, in order for a specific processing of personal data to be lawfully carried out by a public entity, the same must be necessary for the fulfillment of a legal obligation by the data controller or for the execution of a task of public interest or connected to the exercise of public powers and must find its basis in a provision that has the characteristics set forth in art. 2-ter of the Code.

The legislation referred to by the Council, while legitimizing the processing of data relating to the application for admission to free legal aid at the expense of the State, does not provide for the processing by the Order of the authentication credentials for accessing the PEC mailbox in use at the lawyer who uses the portal in question.

Nor can it be considered relevant, for the purposes of assessing the overall conduct of the data controller, what is represented by the Council regarding the fact that "registration is carried out by the data controller both by express consent and for the performance of a task of interest public". This is because consent does not usually constitute a valid prerequisite for lawfulness for the processing of personal data in the public sphere due to the imbalance in the position of the data subjects with respect to the data controller (see recital no. 43 of the Regulation).

Furthermore, it is noted that, based on the documentation acquired in the records, it does not appear that in order to register on the portal in question, consent was required for the processing of the aforementioned personal data.

In any case, the consent invoked by the Order could not have been considered, in the context of the treatment in question, a "manifestation of free will" (Article 4, point 11), of the Regulation) considering that lawyers were led to consider it mandatory the use of the aforementioned portal, based on what is reported in the notice published on the website of the Order, according to which "the filing of all applications [for legal aid at the expense of the State] can only take place through the use of the specific telematic platform".

Nor can the processing of the authentication credentials of the PEC boxes (username and password) used by lawyers be considered authorized as it is not "necessary for the execution of a task in the public interest or connected to the exercise of

public powers vested in it the data controller" (Article 6, paragraph 1, letter e), of the Regulation), since this purpose can be pursued with less invasive means, which do not jeopardize the rights and freedoms of the interested parties (providing, for example , that it is the lawyer himself who autonomously arranges for the aforementioned submission in compliance with the aforementioned sector regulations).

In addition, the treatment of the authentication credentials of the PEC boxes, carried out with the aforementioned methods (with or without archiving the credentials themselves in the alleged "technical cookie"), is in contrast with the principle of "integrity and confidentiality" , pursuant to art. 5, par. 1, lit. f), of the Regulation. This is because the processing, as configured, does not guarantee adequate security of personal data and involves serious and unjustified risks for the rights and freedoms of the interested parties deriving from potential unauthorized access to the PEC box used by the lawyer, which contains personal data, also belonging to particular categories or relating to criminal convictions and crimes (articles 9 and 10 of the Regulation), referring not only to the lawyer himself but also to his clients or to other subjects (lawyers, magistrates, etc.).

Furthermore, in consideration of the habit of many users to reuse the same password, or in any case a very similar password, for accessing a plurality of online services, a possible violation of the aforementioned authentication credentials could also have negative effects in relation to treatments carried out in contexts other than the one in question.

Lastly, the fact that "the design of the portal, including the provision of the request for access credentials to the certified e-mail of the instant defender derive[sse] from a specific design indication by Servicematica, cannot be considered suitable to justify the Order's conduct which represented to the [...] Order the absolute need to obtain the aforesaid data as equally necessary for the correct management of the requests and also highlighted how the aforesaid portal had already been activated with the same precautions and the same technical methods for other legal orders".

In fact, the legislation on the protection of personal data provides that it is up to the data controller to make decisions regarding certain key elements of the treatment itself. The data controller is therefore required to establish the purposes and means of the processing, i.e. the reason and methods of the processing (Article 4, point 7 of the Regulation).

In this regard, the "Guidelines 07/2020 on the concepts of data controller and data processor pursuant to the GDPR", adopted by the European Data Protection Board on the XX, highlight, in fact, that "as regards the definition of means, a distinction can be made between essential and non-essential means. The «essential means» are traditionally and intrinsically reserved to the data controller. [...] "Essential means" means the means strictly related to the purpose and scope of the processing, including

the type of personal data processed ("which data are processed?") [...] Together with the purpose of the processing, the means are also strictly connected to the lawfulness, necessity and proportionality of the processing itself" (see, in part, point 40).

In the light of the foregoing considerations, it is believed that, in the context of the aforementioned portal for the presentation of requests for access to free legal aid, the Bar has illegally processed the authentication credentials of the PEC mailboxes of the lawyers (username and password), in absence of a suitable legal basis, in violation of articles 5, par. 1, lit. a), and 6, par. 1, lit. e), of the Regulation, as well as the principle of "integrity and confidentiality" pursuant to art. 5, par. 1, lit. f), of the Regulation.

3.3 The transparency of the treatment and the information given to the interested parties.

With reference to the different profile relating to the information provided to the lawyers upon registration on the portal, it appears that, at least until the XX (date of the preliminary investigation carried out by the Office), the information necessary to ensure a correct and transparent treatment, as required by articles 5, par. 1, lit. a), and 13 of the Regulation. Moreover, despite the aforementioned registration form, which can be found on the web page "https://...", requesting the "view of the privacy information (information available on the website of the lawyers association)", on this page there was no no link to this information.

Furthermore, the information recalled was not even produced in response to the request for information formulated by the Guarantor. In fact, the Council limited itself to providing the Authority with a list of the information provided ("Identity and contact details of the Data Controller [...]; Contact details of the DPO; Purpose of the processing and legal basis; Processing methods and data retention period; Scope of communication and dissemination; Rights of the interested party; Retention period") without attaching a copy of this information. The Order, therefore, has not demonstrated the fulfillment of the principle of transparency in violation of the principle of accountability pursuant to art. 5, par. 2, of the Regulation.

On the 20th date, the Board represented that, on the aforementioned web page for registering on the portal, a "specific reference to the privacy information notice was introduced, the link of which correctly refers to the information notice prepared by Servicematica", previously not present and has attached "the video prints of the portal accompanied by the indications [...] described" including a disclosure not pertaining to the processing of the personal data in question.

In this regard, the Office has noted that the attached information on the processing of personal data is not suitable for making the treatment in question transparent for the interested parties, in the terms required by art. 13 of the Regulation. This is

because the same information, after having clarified that the company Servicematica "in accordance with the Order of Lawyers for which the service is provided, manages the web portal, processing only the data necessary to process requests", identifies as the owner of the processing of the personal data of the lawyers the same company Servicematica S.r.l..

The identification of the company Servicematica S.r.l. however, as data controller, it does not comply with the definitions provided for by the Regulation (art. 4, points 7) and 8), of the Regulation) which qualify as data controller the subject who, as mentioned above, "singly or jointly with others, determines the purposes and the means of processing personal data; when the purposes and means of such processing are determined by Union or Member State law, the data controller or the specific criteria applicable to his designation may be established by Union or Member State law" and as data controller the subject "who processes personal data on behalf of the data controller" (see the appointment of the company Servicematica S.r.l. by the Order as responsible for data processing carried out within the portal in question, pursuant to article 28 of the Regulation, produced by the Company on XX).

Furthermore, the text of this information is extremely generic and does not contain, in particular, references to the specific treatments carried out through the system and to the legal basis of the treatment, limiting itself generically to providing that "The data are used by the Data Controller to follow up on the contract for the supply of the chosen Service, manage and execute the contact requests forwarded by the interested party, provide assistance, provide information regarding the services related to the profession and fulfill the legal obligations to which the Data Controller is required according to the activity carried out. Under no circumstances does SM Srl resell the personal data of the interested party to third parties or use them for undeclared purposes".

With reference to this information, at a later stage (see documentation of the XX) the Board specified that "the Order provided for the requested response also attaching the privacy information prepared independently by the manager Servicematica s.r.l. and communicated by him […]. With respect to this information text attached to the communication, it is important to highlight that it is not the one relating to the service subject to verification by the Guarantor, but the text of the information relating to the treatment, by Servicematica s.r.l., of the data of its customers to title of independent Data Controller, for its own purposes, usually provided by Servicematica itself when accessing its website. It therefore has no relevance, for the purposes of the ongoing proceedings, as it is a document unrelated to the services and treatments subject to verification by the Guarantor".

In the same note, the Order also represented that "In the original structure of the portal, in fact, it was indicated that the

information was published directly on the Order's website but the presence of a hypertext link to that page has not been confirmed. The aforesaid information, in relation to which users were required to proceed with acknowledgment, has in fact always been contained, and can always be consulted, at the web address https://.... Following the findings of the Guarantor, the therefore proceeded to prepare a hypertext link positioned for access to the portal and within the procedure for registering a new user for the services, which refers directly to the privacy information".

Given this, it should be noted that following further investigations carried out by the Office on the 20th date, it emerged that the portal dedicated to legal aid has been reactivated by the Order and that the new registration form present on this portal does not require the insertion authentication credentials for accessing the lawyer's PEC mailbox. However, it has been noted that the link to the information on the processing of personal data present in the registration form refers to information relating to "online activities [... carried out on the site of the company SM S.r.l.] valid for visitors/users of the site" which indicates the aforementioned company as data controller, with registered office in Venice in via Trieste 158/B. Therefore, this disclosure does not provide any information regarding the specific processing in question.

Therefore, on the basis of the documentation acquired in the records and the declarations made by the data controller, it appears that the Order has not provided the interested parties, when registering on the portal, with information relating to the processing of personal data carried out therein. At first because, despite the registration form found on the aforementioned web page requiring the "view of the privacy information", there was no link to the information on this page, while, currently, there is a link to the " privacy policy" concerning the online activities carried out on the site of the company SM S.r.l., which indicates the aforementioned company as data controller and therefore does not provide information relating to the specific processing carried out on the Portal subject of the complaint.

For all the reasons represented above, the processing implemented by the Order cannot be considered compliant with the principle of "lawfulness, transparency and correctness", since all the information elements envisaged by the Regulation have not been provided to the interested parties (articles 5, par. 1, letter a), and 13 of the Regulation).

3.4 The archiving of information in the user's terminal and access to information already archived.

From the documentation in the documents it emerged that, at least until the date of the twentieth century, when a lawyer registered on the portal in question, the access password to his PEC box was stored, in encrypted form, within an alleged " technical cookie" and, subsequently, upon presentation of an application for admission to free legal aid, the same portal

accessed the password contained within this “technical cookie”.

In other words, the portal archived, in encrypted form, the password for accessing the lawyer's PEC mailbox in the terminal used by the latter and, subsequently, accessed this information in order to transmit the request to the Bar of admission to free legal aid on behalf of the lawyer. This without the lawyer being informed of this circumstance and of the risks that the memorization, albeit in encrypted form, of a password in a cookie can entail in terms of security.

In this regard, it is noted that, since the aforementioned cookie cannot be considered a "technical cookie" - as it is not strictly necessary for the provision of the service (the lawyer being able to autonomously send the digitally signed application from his mailbox PEC, without having to provide the Order with access credentials to the same) -, the storage within this cookie of information not strictly necessary for the provision of the service, and the subsequent access to the same, could have been carried out only at provided that the interested party had given his informed consent pursuant to art. 122 of the Code.

However, the documentation in the documents does not show that methods for collecting this consent were envisaged within the context of the portal in question.

For these reasons, the processing of personal data in question, carried out in the absence of a suitable legal basis in the terms described above, is in violation of art. 122 of the Code.

3.5 Data protection by design and by default.

From the declarations in the documents it also emerged that "in designing the software for free legal aid", the Order evaluated "various ways of presenting the applications and it was agreed to proceed with the electronic submission via PEC and digital signature, seen also the art. 65 of Legislative Decree 7 March 2005, n. 82, a solution that guarantees the authenticity of the document and the certainty of the date of presentation of the application”.

As a preliminary point, it should be noted that the aforementioned legislation establishes that, in order to be valid, applications presented to public administrations electronically must be presented exclusively in the manner provided therein (see Article 65 of Legislative Decree 7 March 2005, No. 82, hereinafter "CAD", in the formulation prior to the amendments made by Legislative Decree No. 76 of 16 July 2020, converted, with amendments, by Law No. 120 of 11 September 2020).

However, the aforementioned provision - while providing, among other hypotheses, that the aforementioned requests, "submitted electronically to the public administrations", are valid "if signed using one of the forms referred to in article 20" of the CAD (i.e. "when a digital signature, another type of qualified electronic signature or an advanced electronic signature has been

affixed to it or, in any case, it is formed, subject to computer identification of its author, through a process having the requisites set by the AgID [...]") - does not presuppose in any way the treatment of authentication credentials (username and password) used by the applicant to access his PEC box by the subjects referred to in art. 2, paragraph 2, of the CAD, being able, in the present case, the lawyer himself to autonomously send the digitally signed application from his PEC box.

It is also noted that, based on the principle of "data protection from the design" (Article 25, paragraph 1, of the Regulation), the data controller must adopt adequate technical and organizational measures to implement the principles of data protection and must integrate the necessary guarantees in the treatment to meet the requirements of the Regulation and protect the rights and freedoms of the interested parties. 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 controller to ensure that they continue to comply with the principles and allow the controller to fulfill the obligations set out in the Regulation (see "Guidelines 4/2019 on Article 25 Data protection from the design and by default", adopted the XX by the European Data Protection Board, spec. points 7 and 39).

It should also be noted that, in accordance with the principle of "data protection by default" (article 25, paragraph 2, of the Regulation), the controller must make, assuming responsibility for them, choices such as to ensure that it is carried out by default by default only the treatment strictly necessary to achieve a specific and lawful purpose. This means that, by default, the controller must not collect personal data that is not necessary for the specific purpose of the processing. Even when using products or services made by third parties, the data controller must carry out a risk assessment and make sure that the functions that have no legal basis or are not compatible with the purposes of the treatment are deactivated (see "Guidelines 4 /2019 on Article 25 Data protection by design and by default", adopted on XX by the European Data Protection Board, spec. points 42, 44 and 49).

Given this, during the preliminary investigation it emerged that the processing of the lawyers' personal data, carried out within the "https://..." portal in order to be able to present the applications for admission to free legal aid, was placed existing by the Order without adopting, from the planning stage and by default, adequate technical and organizational measures and necessary guarantees, aimed at mitigating the risks for the rights and freedoms of the data subjects and guaranteeing treatment that complies with the principles of the Regulation.

In particular, it appears that the Order, in determining the means of the processing in question - which also concerns the

authentication credentials used by lawyers to access their PEC mailbox, which are not necessary for the pursuit of a lawful purpose -, has not adopted adequate measures and guarantees to effectively implement the principles of "lawfulness, correctness and transparency" and of "integrity and confidentiality" (articles 5, paragraph 1, letters a) and f), of the Regulation), also taking into account the high risks for the rights and freedoms of the interested parties deriving from the processing of the aforementioned personal data.

In the light of the foregoing considerations, the processing of the lawyers' personal data was carried out by the Bar in a manner that does not comply with the principles of "data protection by design" and "data protection by default", in violation of art. . 25 of the Regulation.

4. Conclusions.

In the light of the assessments referred to above, taking into account the statements made by the data controller during the preliminary investigation □ the truthfulness of which may be called upon to answer pursuant to art. 168 of the Code □ it should b noted that the elements provided by the data controller in the defense briefs do not allow for overcoming the findings notified by the Office with the act of initiation of the procedure and are insufficient to allow the filing of the present proceeding, not resorting Moreover, any of the cases provided for by art. 11 of the Regulation of the Guarantor n. 1/2019.

Therefore, the preliminary assessments of the Office are confirmed and the unlawfulness of the processing of personal data carried out by the Order is noted, in violation of articles 5, 6, 13 and 25 of the Regulation as well as art. 122 of the Code.

The violation of the aforementioned provisions makes the administrative sanction envisaged by art. 83, para. 4 and 5 of the Regulation, pursuant to articles 58, par. 2, lit. i), and 83, par. 3, of the same Regulation and of the art. 166, paragraph 2, of the Code.

5. Corrective measures (Article 58, paragraph 2, letter d), of the Regulation).

The unlawful conduct held by the Order has not fully exhausted its effects, as, at present, the same has not demonstrated that it has provided the interested parties with adequate and preventive information regarding the processing of personal data requested from lawyers when registering on the portal in question.

It is therefore considered necessary, pursuant to art. 58, par. 2, lit. d), of the Regulation, to enjoin the Order to conform the treatments to the provisions of the Regulation, within and no later than thirty days from the notification of this provision:

- eliminating, from the registration form on the https://... portal, the link to the information on the processing of personal data

currently present;

- providing the interested parties with suitable information regarding the personal data processed as part of the registration procedure on the aforementioned portal through which it is possible to access the services relating to free legal aid activated by the Order (articles 5, paragraph 1, letter a), and 13 of the Regulation).

Pursuant to articles 58, par. 1, lit. a), of the Regulation and 157 of the Code, the Order will have to provide to communicate to this Authority what initiatives have been undertaken in order to implement what is enjoined with this provision, providing an adequately documented response, within and no later than thirty days from the notification of this provision.

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

The Guarantor, pursuant to articles 58, par. 2, lit. i), and 83 of the Regulation as well as art. 166 of the Code, has the power to "impose a pecuniary administrative sanction pursuant to article 83, in addition to the [other] [corrective] measures referred to in this paragraph, or instead of such measures, according to the circumstances of each single case" and, in this context, "the College [of the Guarantor] adopts the injunction order, with which it also orders the application of the ancillary administrative sanction of its publication, in whole or in part, on the website of the Guarantor pursuant to article 166, paragraph 7, of the Code" (art. 16, paragraph 1, of the Guarantor's Regulation no. 1/2019).

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

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

In relation to the aforementioned elements, the delicacy of the unlawfully processed personal data was considered, concerning the authentication credentials (username and password) for accessing the PEC mailboxes of lawyers, moreover in the absence of specific and adequate information.

On the other hand, it was considered that the Order proceeded to suspend the service in question following discussions with the Guarantor, collaborating with the Authority during the preliminary investigation of the present proceeding. It was also noted that there are no previous relevant violations committed by the data controller or previous provisions pursuant to art. 58 of the

Regulation.

Based on the aforementioned elements, evaluated as a whole, it is deemed necessary to determine the amount of the pecuniary sanction, in the amount of 20,000.00 (twenty thousand) euros for the violation of articles 5, 6, 13 and 25 of the Regulation and 122 of the Code, as a pecuniary administrative sanction withheld, pursuant to art. 83, par. 1, of the Regulation, effective, proportionate and dissuasive.

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

Finally, it should be noted that the conditions pursuant to art. 17 of Regulation no. 1/2019 concerning internal procedures having external relevance, aimed at carrying out the tasks and exercising the powers delegated to the Guarantor.

ALL THAT BEING CONSIDERED, THE GUARANTOR

pursuant to art. 57, par. 1, lit. f), of the Regulations, declares the conduct of the Ancona Bar Association described in the terms described in the justification to be unlawful, consisting in the violation of articles 5, 6, 13 and 25 of the Regulation, as well as art. 122 of the Code;

ORDER

pursuant to articles 58, par. 2, lit. i), and 83 of the Regulation, as well as art. 166 of the Code, to the Ancona Bar Association, in the person of its pro-tempore legal representative, with registered office in Corso Giuseppe Mazzini, 95, 60121 Ancona, Tax Code 80012130425, to pay the sum of 20,000.00 (twenty thousand) euros as an administrative fine for the violations indicated in this provision. 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 the term of thirty days, an amount equal to half of the fine imposed;

ENJOYS

to the Order of Lawyers of Ancona:

without prejudice to the provisions of art. 166, paragraph 8, of the Code, to pay the sum of Euro 20,000.00 (twenty thousand) 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 law n. 689/1981;

pursuant to art. 58, par. 2, lit. d), of the Regulation, to conform the treatments to the provisions of the Regulation, by adopting

the corrective measures indicated in paragraph 5 of this provision, within and no later than thirty days from the date of receipt of the same;

pursuant to articles 58, par. 1, lit. a), of the Regulation and 157 of the Code, to communicate to this Authority, providing an adequately documented response, within thirty days of notification of this provision, the initiatives undertaken to ensure compliance of data processing with the Regulation;

HAS

the publication of this provision on the Guarantor's website pursuant to art. 166, paragraph 7, of the Code (see art. 16 of the Guarantor's Regulation no. 1/2019);

the annotation of this provision in the internal register of the Authority, provided for by art. 57, par. 1, lit. u), of the Regulation, of the violations and measures adopted in accordance with art. 58, par. 2, of the Regulation (see art. 17 of Regulation no. 1/2019).

Pursuant to articles 78 of the Regulation, 152 of the Code and 10 of Legislative Decree no. 150/2011, against this provision it is possible to lodge an 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 appellant resides abroad.

Rome, 13 April 2023

PRESIDENT

station

THE SPEAKER

Zest

THE SECRETARY GENERAL

Matthew