[doc. web no. 9039235]

Injunction against the Bari local health authority - 28 June 2018

Register of measures

no. 399 of 28 June 2018

THE GUARANTOR FOR THE PROTECTION OF PERSONAL DATA

IN today's meeting, in the presence of Dr. Antonello Soro, president, of dott.ssa Augusta Iannini, vice president, of dott.ssa Giovanna Bianchi Clerici and of prof.ssa Licia Califano, members and of dott. Giuseppe Busia, general secretary;

CONSIDERING the art. 1, paragraph 2, of the law of 24 November 1981, n. 689, pursuant to which the laws that provide for administrative sanctions are applied only in the cases and for the times considered in them;

NOTING that the Guardia di Finanza, special privacy unit, with report no. 5 of 18 January 2018 (notified on 8 February 2018), which must be understood as fully reported here, contested the local health authority (hereinafter ASL) of Bari, in the person of the pro-tempore legal representative, with registered office in Bari , seafront Starita n. 6, tax code 06534340721, the violation of the provisions of articles 33 and 162, paragraph 2-bis, of the Code regarding the protection of personal data (legislative decree no. 196 of 30 June 2003, hereinafter referred to as the "Code");

NOTING that from the examination of the documents of the sanctioning procedure initiated with the contestation of administrative violation, the following emerged, in summary:

- the Guardia di Finanza carried out an inspection of the ASL of Bari, at the San Giacomo hospital in Monopoli, on 21, 22 and 23 November 2017, as part of the six-monthly inspection program established by the Guarantor;

- during the investigation, during which the various IT applications in use at the facility were examined, it emerged that the credentials for accessing some of them (Hdgold Olivetti, Hospital Cardio, Geos, Gepadial, Armonia, Emodata ) are shared among the employees who use them. It also emerged that, with reference to two systems (Hospital Cardio and Edotto Sist), some employees access them using passwords consisting of less than eight alphanumeric characters;

- on the basis of the aforementioned elements, the Guardia di Finanza drafted the notification of administrative violation no. 5 of 18 January 2018;

NOTING that with the aforementioned report the ASL of Bari was challenged, pursuant to art. 162, paragraph 2-bis, of the Code, the violation of articles 33 et seq. of the Code and the rules of the technical specification referred to in the relative Annex

B);

READ the defensive writings of 5 March 2018, where the following is observed, in summary:

- "with reference to the inspection carried out by the Special Privacy Unit at the San Giacomo Hospital in Monopoli, some workstations not connected (so-called join) to the single corporate domain were subjected to checks. This circumstance is configured as an exceptional case in consideration of the general security policy defined by the company according to which all workstations must be subject to minimum security measures, as governed by articles 33-34 of the Personal Data Protection Code. It should be noted that since 2011, the ASL of Bari has adopted internal regulations for the use and management of company IT and telematic instrumental resources [...]. With reference to the detection of password sharing between operators, it should be noted that the ASL of Bari has always regulated and made all company personnel aware of the issues of protection and confidentiality of personal data. The Regulation referred to above in chapter no. 4 par. 4.2 establishes that the authentication credentials consist of a user identification code (user id), assigned by the U.O.A.S.S.I. [Computer system analysis operating unit], associated with a confidential keyword (password) created by the person in charge which must be memorized, kept with the utmost diligence and not disclosed. It should also be noted that the Company has not implemented a single sign-on for which even access to the domain does not allow the use of the application systems, which manage personal and/or sensitive data, unless after a specific application authentication which requires nominative credentials with diversified authorizations by type of user as certified by application software suppliers.";
- “the omissions detected and contested by the Special Privacy Unit were determined by the behavior of authorized subjects of the Bari Local Health Authority in violation of the company's Internal Regulations, adopted with resolution of the General Manager no. 925 of 16 May 2011, noting in this sense the exclusion of liability of the Data Controller, innocent in the present case and always attentive to the observance of the regulations on the protection of personal data, with always demonstrated ordinary diligence".

CONSIDERING that the arguments put forward are not suitable for determining the closure of the sanctioning procedure initiated with the above dispute for the following reasons:

- it emerges, from the reports of operations carried out during the inspection at the San Giacomo di Monopoli facility, whose organization in terms of security in the processing of personal data falls under the responsibility of the ASL of Bari as the owner of the same processing, a non-episodic violation of the computer authentication rules dictated by articles 33 et seq. of

the Code and by rules nos. 3, 4, 5 and 6 of the technical specification referred to in Annex B) of the same Code;

- this violation, due to its systematic nature, must be attributed to the responsibility of the ASL of Bari, which has not adopted suitable measures to prevent access to the systems from using passwords consisting of a lower number of alphanumeric characters to eight and with the sharing of authentication credentials between multiple data processors;

NOTING, therefore, that the ASL of Bari, on the basis of the considerations referred to above, appears to have committed the violation provided for by art. 162, paragraph 2-bis, of the Code, for having failed to adopt the minimum security measures envisaged by articles 33 et seq. of the Code and by rules nos. 3, 4, 5 and 6 of the technical specification referred to in Annex B) of the same Code;

CONSIDERING the art. 162, paragraph 2-bis, of the Code, which punishes the violation of articles 33 et seq. and the rules dictated by the technical specification referred to in Annex B) of the Code, with the administrative sanction of the payment of a sum from 10,000 to 120,000 euros;

CONSIDERING that, for the purposes of determining the amount of the pecuniary sanction, it is necessary to take into account, pursuant to art. 11 of the law n. 689/1981, of the work carried out by the agent to eliminate or mitigate the consequences of the violation, the seriousness of the violation, the personality and economic conditions of the offender;

WHEREAS, in the present case:

a) in terms of the aspect of gravity with reference to the elements of the extent of the injury or danger and the intensity of the psychological element, the violation is not characterized by specific elements;

b) for the purposes of evaluating the work performed by the agent, the fact that the ASL has not communicated to the Guarantor any measures adopted following the dispute of administrative violation in order to adapt the security measures must be considered in unfavorable terms with current regulatory provisions;

c) about the personality of the perpetrator of the violation, the ASL is burdened by a previous specific sanctioning procedure regarding minimum security measures defined with an order-injunction (provision no. 7 of 10 January 2013);

d) with regard to the economic conditions of the agent, the financial statements for 2017 were taken into consideration;

CONSIDERED, therefore, of having to determine, pursuant to art. 11 of Law no. 689/1981, the amount of the pecuniary sanction, based on the aforementioned elements evaluated as a whole, in the amount of 20,000 (twenty thousand) euros;

HAVING REGARD to the documentation in the deeds;

CONSIDERING the law n. 689/1981, and subsequent modifications and additions;

HAVING REGARD TO the observations of the Office formulated by the Secretary General pursuant to art. 15 of the Guarantor's regulation n. 1/2000, adopted with resolution of 28 June 2000;

SPEAKER Prof. Licia Califano;

ORDER

to the local health authority of Bari, in the person of its pro-tempore legal representative, with registered office in Bari, Lungomare Starita n. 6, tax code 06534340721, to pay the sum of 20,000 (twenty thousand) euros as an administrative fine for the violations indicated in the justification;

ENJOYS

to the same Healthcare Authority to pay the sum of 20,000 (twenty thousand) euros, according to the methods indicated in the attachment, within 30 days of notification of this provision, under penalty of adopting the consequent executive acts pursuant to art. 27 of the law of 24 November 1981, n. 689.

Pursuant to articles 152 of the Code and 10 of Legislative Decree no. 150/2011, opposition to this provision may be lodged with the ordinary judicial authority, with an appeal lodged with the ordinary court of the place where the data controller has his residence, within the term of thirty days from the date of communication of the provision itself or sixty days if the appellant resides abroad.

Rome, 28 June 2018

PRESIDENT

Soro

THE SPEAKER

Califano

THE SECRETARY GENERAL

Busia