Decision No 67 of 8 February 2024

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

At today's meeting, with the participation of Prof. Pasquale Stanzione, President; Prof. Ginevra Cerrina Feroni, Vice-President; Dott. Agostino Ghiglia and Avv. Guido Scorza, Members; and Cons. Fabio Mattei, Secretary-General;

Having regard to legislative decree No 196 of 30 June 2003 (Personal Data Protection Code, hereinafter 'Italian DP Code' or the 'Code') as amended by legislative decree No 101 of 10 August 2018 containing 'Provisions to adapt the national legal system to Regulation (EU) 2016/679 (GDPR)';

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the 'Regulation');

Having regard to the complaint lodged by a German national with the Baden-Wurttemberg supervisory authority regarding the allegedly unlawful processing of data concerning him by Gilmar Divisione Industria S.p.A., which had sent him the password for accessing the website www.gilmarbox.it in unencrypted format in the e-mail confirming registration for that website;

Taking account of IMI Art. 56 procedure No 66422 that was opened by the Baden-Wurttemberg (BW) SA insofar as an instance of cross-border data processing was at issue, which was communicated to the other EEA SAs on 8 May 2019;

Taking account that the Italian SA accepted to act as the lead supervisory authority in the said procedure since the controller has its main establishment in Italy;

Having regard to the draft decision which was shared with the other supervisory authorities concerned via the IMI platform on 20 May 2020 and was not the subject of any relevant and reasoned objections, whilst comments were submitted by the BW SA as well as by the French SA (CNIL). In particular, the BW SA requested that a call be included on the controller to rely preferably on other password storage techniques – such as Argon 2, or bcrypt, or PBKDF2 – which were considered to be even more secure; though endorsing the proposed decision to close the proceeding, the French SA requested that reference should be made therein to the circumstance that personal data protection legislation had been infringed, however the controller had remedied the infringement following the action taken by the Garante;

Having regard to the revised draft decision (RDD) as shared with the other supervisory authorities concerned on 11 December 2020, which included amendments made as a result of the comments by the BW SA and was not the subject of any relevant and reasoned objection by the other CSAs. In particular, the BW SA agreed to the RDD, whilst the French SA reiterated the comments made regarding the Draft Decision, once again underlining the need to specify the above circumstance;

Having regard to the new RDD as shared with the other supervisory authorities concerned on 8 November 2023, including amendments on the basis of the comments by the French SA, which was not the subject of any relevant and reasoned objection by the other supervisory authorities and has become accordingly binding pursuant to art. 60(6) of the Regulation;

Having regard to the records on file;

Having regard to the considerations submitted by the Secretary General in pursuance of Section 15 of the Garante's Regulations No 1/2000;

Acting on the report submitted by Prof. Ginevra Cerrina Feroni;

WHEREAS

1. The complaint and the relevant inquiries

The case originates from the complaint lodged with the Baden-Wurttemberg SA by [redacted] against the allegedly unlawful processing of his personal data by Gilmar Divisione Industria S.p.A., which had sent him the password for accessing the website www.gilmarbox.it in unencrypted format in the e-mail confirming registration for that website.

This had led the complainant to question the adequacy of the security measures implemented to protect personal data.

Having accepted to act as the lead supervisory authority in the case at issue since the controller has its main establishment in Italy, on 16 July 2019, the Garante sent a letter to Gilmar Divisione Industria S.p.A. to inquire about the technical and organisational measures in place to ensure the security of the processing at issue with particular regard to the following:

- a description of the registration procedure implemented for the www.gilmarbox.it website, including the reasons why the password chosen by the user is sent to the latter within the e-mail confirming registration;
- a description of the measures taken for storing the passwords of registered users including the encryption techniques (such hashing and salting) applied to protect them.

The controller replied to the said request for information by a letter dated 16 September 2019, where it explained that the procedure did envisage including the password chosen by users in the e-mails sent to confirm completion of their registration. Each password was subsequently stored securely in the company's database in hashed format using the SHA256 algorithm and a different salt for each user.

Additionally, the controller explained that it had decided to enhance security of processing as a consequence of the complaint at issue by refraining from including the users' passwords in the e-mails confirming their registration.

In this respect, the Garante took note of the submissions made by the company also in the light of Section 168 of the Code, and shared a draft decision with the other supervisory authorities concerned to close the proceedings without taking any corrective measures against Gilmar Divisione Industria S.p.A. .

2. Assessment by the Garante

The Garante took account of the findings of the investigation, that it was an isolated case and that the controller proactively proceeded to modify its procedure by abstaining from entering the user's password in the registration confirmation e-mail and by implementing encryption-protected password storage mechanisms – although the controller did infringe personal data protection legislation in the one case that is the subject of the current complaint. Accordingly, the Garante closes the proceeding at hand without imposing any corrective or fining measures pursuant to Article 58(2) of the Regulation, taking into account that its intervention '*during the handling of the complaint led the controller to stop the infringement and fully satisfy the complainant's claim'.*

The Garante carried out *'a careful assessment of the circumstances of the complaint as a whole, in order to keep the same level of guarantees afforded to the data subjects'* in line with Guidelines 2/2022 on the application of Article 60 of the General Data Protection Regulation, as adopted by the EDPB on 14.5.2022 (paras. 232, 233, 234).

This decision is adopted by the Garante pursuant to Article 60(7) of the Regulation in its capacity as the lead supervisory authority and is notified to the controller pursuant to the aforementioned Article, whereby the controller is invited to continuously assess and update security standards for the relevant processing.

Under Article 60(7) of the Regulation, the supervisory authority of Baden-Wurttemberg shall inform the complainant of this decision in its capacity as complaint-receiving supervisory authority.

BASED ON THE FOREGOING PREMISES, THE GARANTE

Taking note of the feedback that was provided by Gilmar Divisione Industria S.p.A. regarding the security measures in place, which were found to have been enhanced in the course of the proceeding at issue, as well as of the said company's active cooperation,

a) Closes the proceeding at hand within the meaning of Section 143(3) of the Code and Sections 11(1)(d), 14 and 18 of the Garante's Internal Regulation No 1/2019 concerning internal procedures having external impact as related to discharge of the tasks and exercise of the powers committed to the Garante per la protezione dei dati personali;
b) Calls upon Gilmar Divisione Industria S.p.A., VAT No 03225310402, under Article 57(1)(d) of the Regulation to continuously assess and update its standards to ensure security of processing activities. Furthermore, it is highlighted that, although the system in place affords adequate security, there are other password storage techniques (such as Argon 2, especially, or bcrypt, or PBKDF2) that are considered even more secure.

Under Article 60(7) of the Regulation, this decision shall be notified to the controller, who may challenge it under the terms of Article 78 of the Regulation as applied jointly with Section 152 of the Code and Section 10 of legislative decree No 150 of 1 September 2011 by

lodging an appeal with the court of the place where the controller is resident or has an establishment or else with the court of the data subject's place of residence by thirty days from notification hereof, or by sixty days if the appellant is resident abroad.

Under Article 60(7) of the Regulation, the complaint-receiving supervisory authority shall inform the complainant on this decision.

Rome, 8 February 2024

THE PRESIDENT

THE RAPPORTEUR

THE SECRETARY GENERAL