Record of decisions No 338 of 20.10.2022

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

During today's meeting, attended by 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 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the 'Regulation');

Having regard to the personal data protection code, containing provisions to adapt the national legal system to Regulation (EU) 2016/679 (legislative decree No 196/2003 as amended by legislative decree No 101/2018) (hereinafter the 'Code');

Having regard to the preliminary personal data breach notification as subsequently supplemented and communicated pursuant to Article 33 of the Regulation, whereby Davide Campari Milano NV (hereinafter 'DCM') stated they had been the subject of a ransomware-type attack;

Whereas the security checks performed by DCM allowed establishing that the attack in question had resulted into a violation of the availability of data and systems and that the attackers had unlawfully exfiltrated about 260 GB of data including personal data;

Whereas DCM is a multinational corporate group having its registered office in the Netherlands but its main establishment in Italy; whereas the Garante is accordingly competent for handling the personal data breach in question;

Whereas the controller declared that the data affected by the breach concerned data subjects in several EU MS, in particular from Austria, Belgium, France, Germany, Greece and Spain, as well as in other non-EU countries;

Whereas DCM declared it had taken steps to notify the breach to all the other competent SAs through the individual group companies in each of the EU MS concerned;

Whereas DCM declared that the categories of data subjects affected by the breach included employees and their families, former employees, customers, shareholders, suppliers, and commercial partners (including journalists); whereas DCM declared that the personal data affected by the breach included first and last names and contact details and – with regard to current and former employees – the data processed in the course of the employment relation such as IDs, trade union membership, health information;

Whereas the security checks regarding the breach as submitted to the Garante showed that the attack had been organised and carried out by a highly organised

criminal group with a high-profile damage potential, capable to dodge the security measures in place; whereas, more specifically, the analysis of access logs showed that the DCM's network had been accessed by relying on legitimate VPN (Virtual Private Network) access credentials that had been stolen from a consultant working for an external company, and that the unauthorised as well as undetected access had allowed identifying and exploiting an unpatched vulnerability of a domain controller server system and thereby obtaining administrator privileges over DCM's IT network as a whole;

Whereas the said analysis found that no security patches had been applied to the breached server, which had been left accordingly exposed to IT attacks;

Whereas the failure to apply security patches was not due to inadequate technical and organisational security measures as deployed by the controller, since it resulted rather from a human error (the other servers that were similar to the breached one in terms of their configuration and functions did bear the necessary security patches);

Whereas about 260 GB of data were exfiltrated and both systems (virtual machines) and data underwent malicious encryption with a view to extortion against DCM;

Whereas the controller declared that the individuals 'potentially' concerned by the breach numbered about 10,000 but it specified that such number 'was an excess estimation […] on a prudential basis' and that 'certain numerical data are hard to determine, since the type of attack […] only allows quantitative estimates' whilst it proved impossible 'to establish which and how many data were impacted by the attack both in terms of breach of confidentiality following exfiltration and in terms of a temporary loss of data availability following encryption, it being impossible to determine which data was affected by which action';

Whereas the controller deactivated and isolated the systems concerned immediately it became aware of the attack in progress so as to terminate the violation, proceed with the required security checks and undertake data and system recovery operations;

Noting that the controller, in countering the attack, implemented additional harderning measures for security systems and policies and relied upon security assessments provided by third-party companies specialising in IT security;

Whereas the controller declared it had simultaneously carried out searches in order to verify whether the unlawfully exfiltrated data had been disseminated on the Internet;

Whereas DCM declared as for the impact produced by the temporary loss of data availability that 'basically all of the personal data concerned by the breach could be recovered and restored; only in a residual number of cases was it not possible to recover the data, which anyhow relate only to the 24 hours prior to the incident';

Whereas DCM declared as for the impact produced by the breach of data confidentiality that 'the criminals published [on the homepage of their website] the contact details taken from the Active Directory […] along with a few screenshots of the exfiltrated files including IDs, finance documents and a few contracts' as well as links to files on the so-called dark web 'which could not be downloaded […] in order to analyse their contents'; however, those files had been

exfiltrated mostly 'from a server located in the USA […] and related to the activities of the American subsidiary [in whose respect] a limited amount of data concerned European citizens';

Noting that, as of the date hereof, the web page publishing parts of the data that had been unlawfully exfiltrated from DCM's systems is no longer reachable, and that the attempts to download the data the said criminal group had allegedly published on the dark web proved unsuccessful;

Noting however that the Internet Archive service – this being a non-profit digital library intended to collect screenshots of the WorldWideWeb to document its evolution – still allows, as of the date hereof, viewing a copy of the webpage publishing parts of the data that had been unlawfully exfiltrated from DCM's systems including personal data such as first and last names, job positions, corporate emails and, in a few cases, corporate phone numbers relating to 191 German data subjects – of whom about ten were external consultants –, 135 French data subjects – of whom about ten were external consultants –, 1122 Italian data subjects – of whom about 115 were external consultants –, the copy of the ID relating to an Italian national, and other accounting, contractual or financial documents that were irrelevant under the terms of personal data protection law;

***

Having regard to the communications sent to data subjects via various avenues including a press release that was emailed between 6 and 10 November 2020 to each employee of the group as well as public communications that were made available on the group's portal and in a dedicated section for suppliers, shareholders, former employees and customers;

Finding accordingly that the company complied with the obligations set out in Articles 33 and 34 of the Regulation as for notification of the Garante and communications to data subjects;

Having regard to the declarations made by DCM to the effect of having notified the personal data breach to each of the competent SAs in each of the EU MS concerned by the said breach; having regard as well to the relevant communications to data subjects, which were drafted in the languages spoken in each of the countries concerned;

***

Having regard to the procedure initiated on 3 February 2021 by the Spanish SA on the IMI (IMI A56ID No 177779) under the terms of Article 56 of the Regulation in order to identify the lead supervisory authority (LSA) and the supervisory authorities concerned (CSAs) following the notification that had been given by Davide Campari SA (a Spanish company belonging to the relevant group) in respect of the breach at issue;

Noting that the Italian SA accepted to be the lead supervisory authority (LSA) on 19 February 2021 within the framework of the said procedure, on the basis of the foregoing considerations concerning the controller's main establishment;

Whereas the Garante had already started fact-finding activities regarding the notification of the personal data breach it had received in November 2020;

Having regard to proceeding No 193170 in IMI's Case Register as opened by the Italian SA and to the informal consultation procedure launched on the IMI pursuant to Article 60 of the Regulation on 14 April 2021 (IMI A60IC No 193181), whereby the Garante informed all the other CSAs about the outcome of the said fact-finding activities;

Having regard to the draft decision that was submitted to the other supervisory authorities concerned on 5 November 2021 (IMI A60DD 337611);

Having considered the comments made by the Baden-Wurttemberg SA on 25 November 2021, which concerned the need for the decision to also recall the advisability of implementing two-factor authentication;

Noting that the Italian SA had already covered the above issue in its draft decision and that it accordingly replied to all the concerned SAs by explaining the considerations set out therein without amending the draft decision in any manner (see IMI A60 Informal Consultation Procedure No 373958 of 2 March 2022);

Whereas it was necessary to await closure of the informal consultation prior to proceeding with the final approval of this decision, which closure took place on 2 September 2022;

***

Whereas the controller implemented adequate technical and organisational measures to terminate the security breach in progress and took steps to mitigate its possible adverse effects on data subjects;

Whereas the controller implemented additional technical and organisational measures enhancing the overall security level of its IT infrastructure and thereby reducing the likelihood for similar breaches to occur in future;

Whereas in the light of the comprehensive assessment of the facts submitted to the SA's consideration, the elements acquired and the foregoing analysis, the personal data breach was handled appropriately by the controller and there are no grounds for imposing a reprimand or an administrative fine under the terms of the Regulation;

Whereas DCM addressed the personal data breach in an accountable as well as effective manner, and no infringements could be found either in handling the personal data breach (see Articles 33 and 34 of the Regulation) or in ensuring data security (see Article 5(1)(f) and Article 32 of the Regulation);

Noting, however, that a few personal data are still visible on the Internet, albeit to a residual extent, via the Internet Archive service;

Finding accordingly that it is necessary to order DCM to take all possible steps in order to ensure that any residual copies of the data at issue are withheld from public availability, and to notify the Garante hereof within 30 days of receipt of this decision;

Finding it necessary to communicate this draft decision to the other CSAs via the IMI in pursuance of Article 60 of the Regulation;

Having regard to the documents on file;

Having regard to the considerations made by the Secretary General pursuant to Section 15 of the Garante's Internal Regulations 1/2000 of 28 June 2000;

Acting on the report submitted by Guido Scorza;

Based on the foregoing premises, the Garante

Orders the controller, Davide Campari Milano NV, having its main establishment in Italy, via F. Sacchetti 20 – 20099 Sesto San Giovanni (MI),

a) to take all possible steps in order to ensure that the residual copies of the personal data that were unlawfully exfiltrated and are as of now accessible on the Internet are withheld from public availability;
b) to provide feedback to the Garante regarding the activities under letter a) above within 30 days of the receipt hereof.

Regarding all the remaining issues, the Garante is closing the IMI procedure without taking further action in respect of the controller since data subjects were informed timely, the IT attack was contained, and the controller may in no way be held accountable for negligent behaviour – in the light of the foregoing considerations.

Under Article 78 of Regulation (EU) 2016/679 and Section 152(1-a) of the Code, this decision may be challenged before the competent judicial authority within thirty days of the date of its communication.

Rome, 20 October 2022

THE PRESIDENT

THE RAPPORTEUR

THE SECRETARY GENERAL