AUTORITÀ GARANTE PER LA
PROTEZIONE DEI DATI PERSONALI

Register of Measures
no. 19 of 6 July 2021

SAN MARINO DATA PROTECTION AUTHORITY

THE BOARD

In its sitting of 6 July 2021, which was attended by Mr. Nicola Fabiano, President, Mr. Umberto Rapetto, Vice-President, Ms. Patrizia Gigante, Member of the Board and Ms. Maria Sciarrino, Director.

HAVING REGARD that, on 8 April 2021, this Authority received a report jointly signed by Mr. ———————

HAVING REGARD to Law no. 171/2018 on the protection of natural persons with regard to the processing of personal data, in particular Articles 4, 5, 35, 58, 59, 72 and 73;

NOTING that in said report the above-mentioned ——— indicated that they had learned of the unauthorised disclosure of sensitive data relating to them and that such "data have allegedly been unlawfully taken from their respective social network profile ("Facebook")";

NOTING, moreover, that with the aforementioned report the above ——— requested this Authority to take measures "in order to verify any violations of Law no. 171/2018, or the commission of any other offences to our detriment that the Authority may identify";

NOTING that the fact that the unauthorised disclosure of personal data allegedly unlawfully extracted from the accounts of users registered on the social networking platform "Facebook" has been widely circulated on the Internet;

CONSIDERING, therefore, that Law no. 171/2018 *"guarantees that the processing of personal data respects the data subject's fundamental rights and freedoms and human dignity, with particular regard to confidentiality, personal identity and the right to the protection of personal data"* and that *"everyone shall have the right to the protection of personal data relating to him or her"* (Article 1, paragraphs 2 and 3);

HAVING REGARD to its measure no. 4/2021 issued on 9 April 2021 and notified to the company "**Facebook Ireland Ltd.**" with registered office in **4 Grand Canal – Square - Grand Canal Harbour - Dublin 2 Ireland**, and to the company "**Facebook Inc.**" with registered office in **1 Hacker Way, Menlo Park, CA 94025, United States of America** on 26 April 2021 - received on 19 May 2021 - and on 26 April 2021 – received on 14 May 2021, respectively- which, among other things, in point b) ordered as a matter of urgency, pursuant to Art. 59, paragraph 2, letter e), of Law 171/2018, "*to notify by appropriate means all the persons concerned of the data breach within 10 (ten) days of receipt of this measure*";

DIPARTIMENTO
REPUBBLICA DI SAN MARINO

Translated by Gianluca Bizzocchi
Foreign Affairs Department

CONSIDERING the preliminary investigation carried out and the clarifications received by the Office of the Data Protection Authority from the company Facebook Ireland Ltd. only;

CONSIDERING that the company Facebook Ireland Ltd., acting as data controller (while the company Facebook Inc. acts as data processor), admits and acknowledges that in the period between January 2018 and September 2019 personal data of users of the Facebook platform were extracted by means of a computer technique called "scraping";

CONSIDERING that Facebook stated that the use of scraping is not supported by any detailed technical report, nor by the outcome of rigorous internal investigations that clearly demonstrates that the extraction of personal data leads back to the aforementioned method;

CONSIDERING that, even admitting that a method comparable (certainly not to the extent) to *scraping* was used, the large amount of data collected by third parties and the consequent traffic volume generated to transfer information from the Facebook servers to the computers of the presumed scrapers would have been immediately recognized as a dangerous anomaly and would have had to trigger preventive and defensive mechanisms to avoid the perpetration of any action potentially harmful for the confidentiality of the personal data of the platform users;

CONSIDERING, the document received by the Office of this Authority on 27 May 2021 on page 6 states verbatim: *Facebook Ireland believes that the Scraped Data Set was compiled between January 2018 and September 2019 ("Relevant Period") through phone number enumeration using scraping using contact discovery features on Facebook platforms ("Relevant Features"),*". Moreover, a footnote states verbatim "*namely, Messenger Contact Importer, Facebook Contact Importer and Facebook Search*";

CONSIDERING,, moreover, that in the same document Facebook Ireland Ltd. States verbatim: "... we understand that this refers to scraped Facebook user data, which was made publicly available in an unsecured database earlier this year, as reported in news articles in April 2021 (the "Scraped Data Set")."

CONSIDERING, therefore, that the companies Facebook Inc. and Facebook Ireland Ltd. were fully aware of the risks associated with the possible extraction of personal data through *scraping*, as confirmed by the fact that they describe it in the documents sent;

CONSIDERING that Facebook, on its own website at https://www.facebook.com/help/463983701520800, states that "*Rate limits caps the number of times anyone can interact with our products in a given amount of time*" and "*Data limits keep people from getting more data than they should need to use our products normally*"), and, however, what happened in this case has showed the substantial inadequacy of the security measures allegedly adopted by the data controller;

Translated by Gianluca Bizzocchi
Foreign Affairs Department

CONSIDERING, therefore, that Facebook Ireland Ltd. - beyond the period of reference of the events, which, in the opinion of this Authority, due to the results of the investigations carried out, date back to the first months of 2021 - has explicitly acknowledged that personal data were extracted by third parties (by means of an alleged and unproven action of scraping) and that this acknowledgement must be considered as a admission;

CONSIDERING that, due to their nature, the activities perpetrated through scraping and/or by any other system aimed at the undue massive extraction of data and the subsequent disclosure through the dissemination of the dataset of personal data - as in this case - are to be considered illegal;

CONSIDERING that Article no. 33 of Law no. 171/2018 states:

Art.33 - (Treatment processing)

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures, to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 41 or an approved certification mechanism as referred to in Article 43 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by special laws.

CONSIDERING, therefore, that the data controller and data processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk;

CONSIDERING that the activities of extraction of personal data from the Facebook platform through scraping or any other aggressive means, as acknowledged by Facebook Ireland Ltd, clearly shows that such company, has not taken adequate measures, as required by Article 33 of Law no. 171/2018, shall implement adequate technical and organizational measures to reduce at least the risk arising from illegal activities of extraction of personal data through scraping or any other technique suitable to illicitly extract massive amount of date, nor has it provided evidence of taking specific measures despite publicly providing relevant assurances;

CONSIDERING that, as described in the clarifications received by this Authority, both companies Facebook Inc. and Facebook Ireland Ltd. should have taken the appropriate measures pursuant to the aforementioned Article no. 33 of Law 171/2018 because they were already fully aware of the concrete risks of cyber attacks in particular (but not only) through scraping;

CONSIDERING that Law 171/2018 defines "dissemination" as follows: *"giving knowledge of personal data to non-specified entities, in whatever form, also by making them available or by consultation"* (Article 2, paragraph 1, letter cc);

CONSIDERING that, pursuant to Law no. 171/2018 processing means *"the dissemination or any other form of making available of personal data"* (Article 2, paragraph 1, letter b);

CONSIDERING that, in accordance with Law no. 171/2018, the principles relating to processing of personal data shall be respected (Article 4);

CONSIDERING that, pursuant to Law no. 171/2018, *"processing shall be lawful only if and to the extent that at least one applies"* of the conditions laid down in Article 5 is applied;

CONSIDERING, therefore, that the extraction of personal data of Facebook's platform users through scraping was the obvious consequence of the failure of Facebook Ireland Ltd. and Facebook Inc. to take appropriate measures to avoid what happened;

CONSIDERING that what happened and - we reiterate - confirmed by Facebook Ireland Ltd. itself, entails the infringement of Article 33 of Law no. 171/2018 with the consequent

Translated by Gianluca Bizzocchi
Foreign Affairs Department

application of the related administrative fine pursuant to Article 72, paragraph 1 of Law no. 171/2018;

CONSIDERING that Facebook Ireland Ltd. and Facebook Inc. have not communicated to this Authority that they have in any case subsequently adopted specific actions and this must be taken into account by this Authority to assess the elements indicated in Article 73, paragraph 2, with specific reference to letter c);

CONSIDERING that letter b) of measure no. 4/2021 adopted by the Data Protection Authority is to be revoked;

CONSIDERED that for the imposition of fine, pursuant to Article 73, paragraph 2, this Authority has given due regard to the following circumstances:

With regard to letter a) *"the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them"*, on the basis of the investigations carried out, this Authority believes that, within its own jurisdiction, the number of data subjects affected is high, and that what happened is not only extremely serious, but lacking specific information from the companies Facebook Inc. e Facebook Ireland Ltd. it is plausible that even today there is a risk that personal data may be extracted by through scraping.

With regard to letter b) *"the intentional or negligent character of the infringement"*, this Authority considers that the conduct of Facebook Inc. and Facebook Ireland Ltd. is to be considered as negligent, having failed to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

With regard to letter c) "*any action taken by the controller or processor to mitigate the damage suffered by data subjects*", this Authority refers to the documentation sent by the company Facebook Ireland Ltd. from which, however, the adoption of any measure to mitigate the damage suffered by the data subjects does not emerge.

With regard to letter d) *"the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 27 and 33"*, this Authority considers that the companies Facebook Inc. and Facebook Ireland Ltd. are fully liable, each for its respective role, for failure to adopt technical and organizational measures at least to mitigate the risk of personal data extraction through scraping.

With regard to letter f) *"the degree of cooperation with the Data Protection Authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement"*, this Authority has positively assessed the conduct of Facebook Ireland Ltd. in sending documents, although the conduct of Facebook Inc. should be criticized, because responding *"to the*

Authority as a matter of courtesy to confirm its position" as results in the documents submitted by Facebook Ireland Ltd. is not correct. Indeed, this Authority, not only has not received any response from Facebook Inc. but considers it wrong and irregular to claim to be responding to a measure issued (no. 4/2021) *"as a matter of courtesy"*, given that, pursuant to Art. 72, paragraph 2, letter d) non-compliance with an order ... of the Authority is considered an infringement subject to the highest fine provided for by law.

With regard to letter g) *"the categories of personal data affected by the infringement"*, this Authority points out that these categories include mainly "common" personal data, and do not include - as a result of the investigation - special categories of data and personal data relating to criminal convictions and offences.

With regard to letter h) *"the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement"*, this Authority became aware of the infringement following a report by San Marino citizens, although the companies Facebook Inc. and Facebook Ireland Ltd. were fully aware of what had happened and of the relevant consequences and, however, did not communicate the facts to this Authority.

With regard to letter i) *"where measures referred to in Article 59, paragraph 2 have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures"*, this Authority notes that measure no. 4/2021 had already been issued but out of the two addressees - namely Facebook Inc. and Facebook Ireland Ltd. - only the company Facebook Ireland Ltd. partially complied with it, by only providing clarifications to this Authority, while not complying with the urgent request for notification to the persons concerned as provided for in letter b) of the aforementioned measure. Facebook Inc. has not complied with the measure issued, not even by sending clarifications;

Therefore, HAVING ESTABLISHED the need, pursuant to Article 59, paragraph 2, letter d), of Law 171/2018, to order the company "**Facebook Ireland Ltd.**" in the person of its pro-tempore legal representative with legal office in **4 Grand Canal – Square - Grand Canal Harbour - Dublin 2 Ireland**" and to the company "**Facebook Inc.**" in the person of its pro-tempore legal representative with legal office in **1 Hacker Way, Menlo Park, CA 94025, United States of America**, as the data controller and data processor, respectively, to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk, thus minimising the risk arising from activities of personal data extraction including through scraping.

Moreover, HAVING ESTABLISHED the need, pursuant to Article 59, paragraph 2, letter i) of Law 171/2018, to impose to the company "**Facebook Ireland Ltd.**" in the person of its pro-tempore legal representative with legal office in **4 Grand Canal – Square - Grand Canal**

Translated by Gianluca Bizzocchi
Foreign Affairs Department

Harbour - Dublin 2 Ireland" and to the company "**Facebook Inc.**" in the person of its pro-tempore legal representative with legal office in **1 Hacker Way, Menlo Park, CA 94025, United States of America**, as the data controller and data processor, respectively, the fine provided for in Art. 72, paragraph 1 of Law 171/2018 for the infringement of Art. 33 of the same Law.

CONSIDERING that the fine for the aforementioned infringement of Article 33 of Law 171/2018, in application of the circumstances indicated in Article 73, paragraph 2, and in light of the assessments made to impose the fine, amounts to EUR 4,000,000 (EUR four million/00).

Therefore, in the light of the above and having regard to the documents on file,

SAN MARINO DATA PROTECTION AUTHORITY

REVOKES

letter b) of its measure no. 4/2021;

ORDERS

the company "**Facebook Ireland Ltd.**" in the person of its pro-tempore legal representative, with legal office in **4 Grand Canal – Square - Grand Canal Harbour - Dublin 2 – Ireland** and the company "**Facebook Inc.**" in the person of its pro-tempore legal representative, with legal office in **1 Hacker Way, Menlo Park, CA 94025, United States of America**, as data controller and data processor respectively, pursuant to Art. 59, paragraph 2, letter d) of Law 171/2018, to immediately take without delay appropriate technical and organizational measures to ensure a level of security appropriate to the risk, thus minimising the risk arising from activities of personal data extraction including through scraping, and consequently report to this Authority within seven days.

ORDERS

the company "**Facebook Ireland Ltd.**" in the person of its pro-tempore legal representative, with legal office in **4 Grand Canal – Square - Grand Canal Harbour - Dublin 2 – Ireland** and the company "**Facebook Inc.**" in the person of its pro-tempore legal representative, with legal office in **1 Hacker Way, Menlo Park, CA 94025, United States of America**, as data controller and data processor respectively, pursuant to Art. 59, paragraph 2, letter i) of Law 171/2018 and in the light of the reasons set out in the introduction to this measure, to pay - jointly and severally - EUR 4,000,000 (four million euros/00) as an administrative fine for the infringements indicated above;

ORDERS

the aforesaid companies to pay, jointly and severally, 4,000,000 (four million) euro, for the reason above, within 30 (thirty) days of notification of this measure.

Payment of this fine shall be made by wire transfer:

Translated by Gianluca Bizzocchi
Foreign Affairs Department

- IBAN SM 81 K03225 09800 000010006039
- Ecc.ma Camera Repubblica di San Marino
- Area Code 225
- Purpose 592
- **Please note in the wire transfer number and date of the measure**

The Authority shall be informed of the payment of the administrative fine by receiving proof of payment to the Office of the Data Protection Authority.

ORDERS:

to record this measure in the Authority's internal register and to publish it on the Authority's website.

Pursuant to Article 69 of Law no. 171/2018, an objection against this measure may be lodged with the ordinary judicial authority by a judicial appeal in accordance with Article 70 of Law no. 171/2018. The objection shall not suspend the enforcement of the relevant measure.

Worth specifying is that failure to promptly respond to the request pursuant to Article 59 shall be punished with the administrative fine referred to in Article 72, paragraph 2 letter d) of Law no. 171/2018.

San Marino, 6 July 2021

Director of the Office **The Board**

Translated by Gianluca Bizzocchi
Foreign Affairs Department