Bld. Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poştal 010336, Bucureşti ; Tel. +40.31.805.9211; Fax:+40.31.805.9602 www.dataprotection.ro; e-mail: anspdcp@dataprotection.ro

Nr. 59/22.05.2024

Decision

Following the investigation performed at Hyllan Pharma SRL

The National Supervisory Authority for Personal Data Protection, with the headquarters in 28-30 G-ral Gheorghe Magheru Blvd., District 1, post code 010336, Bucharest, legally represented by Ancuța Gianina OPRE, President, **issues this decision against Hyllan Pharma SRL**, with the headquarters in Bucharest, 11A Turturelelor Street, 2nd Floor, sole registration code 21293833, registered with the Trade Registry under no. J40/4681/2007, legally represented by [redacted], as director and [redacted], as data protection officer.

Considering the following:

I. Premises

The personal data security breach notifications received based on Article 33

Hyllan Pharma SRL notified a breach of the personal data security by filling in the form for the breach of the personal data security provided under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), registered with the National Supervisory Authority for Personal Data Processing under no. 831/13.01.2023.

Hyllan Pharma SRL notified a breach of the personal data security by filling in the form for the breach of the personal data security provided under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), registered with the National Supervisory Authority for Personal Data Processing under no. 894/16.01.2023.

Considering the above, ANSPDCP started an investigation at **Hyllan Pharma SRL,** through address no. 3770/23.02.2023.

Following the answer submitted through letters no. 4532 of 07.03.2023 and no. 4557 of 07.03.2023, the National Supervisory Authority for Personal Data Processing (hereinafter referred to as "ANSPDCP") acted as lead supervisory authority (LSA) in this case, given that this company has the main establishment in Romania, by introducing within the application "Internal Market Information System" a notification based on Article 56, registered under no. 561108, in order to inform the supervisory authorities from the other Member States of the European Union.

We present below a summary of the security incident and the results of the investigation performed by ANSPDCP in this case.

I. Description of the case:

Within the period 06.01.2023 – 10.01.2023, an illegal/unauthorized access to the data of a number of 24 clients of **HYLLAN PHARMA SRL** that bought online products via four websites was found. The infrastructure for the storage of the data is managed through the processor **ROMARG SRL**.

An unauthorized person accessed in an unauthorized way the database of **HYLLAN PHARMA SRL,** by adding an information structure from a folder that was collecting the card data of the data subjects. The collection was performed by the hacker by creating a fraudulent page that further

redirected to NETOPIA a part of the data, but also to the e-mail address **ahmadgeniius@outlook.com**.

The compromised data are: **first name, last name, address, city, country, email, card number, card name, expiry date and CVC.**

From the preliminary assessment of the case, the controller concluded that the subject matter is a malware attack php.malware.fopo type. This malware type php.malware.fopo (php object injection) is a form of malware that is injected within the web applications written in php. and which spreads through the exploitation of the vulnerabilities from the web applications or through some phishing type attacks.

Within the personal data security breach notification form submitted by **Hyllan Pharma SRL,** under section "Technical and organisational measures taken (or following to be taken) by the controller", the following are mentioned:

1. The application of security patches: it is important to maintain the web applications and operating systems updated in order to benefit from the latest security patches. This can help to the closure of any known vulnerabilities that could be used by the attackers in order to exploit the system.
2. The use of a security software: the installation and use of a security software, such as a firewall or an antivirus can help to the prevention of the unauthorized access to the systems and to the detection and elimination of the malware software.
3. The implementation of data access rules: the implementation of the data access rules can help to the limitation of the access solely to the authorized persons and the limitation of the access to sensitive data.
4. The use of strong passwords and of the two-steps authentication: the use of a strong password and of a two-steps authentication method, such as a verification code provided via SMS, can help to the protection of the authentication data. Strong passwords should contain at least 8 characters, that shall contain uppercase letters, lowercase letters, numbers and special characters. The two-steps authentication adds an additional security level, because even if someone finds the passwords, he/she cannot access the account without the verification code.
5. The training of the employees: it is important to train the employees on the cybernetic risks and on how to avoid the accessing of dubious websites or the download of malware software.
6. The performance of penetration test regularly: the performance of penetration tests regularly can help to identify the vulnerabilities and take the necessary measures in order to remedy them.
7. The implementation of backup and disaster recovery rules: the implementation of backup and disaster recovery rules can help to the protection of the data in case of a security breach and their recovery in case of a data loss.
8. The use of an injection type protection solution against the attacks.
9. The implementation of a monitoring system: the implementation of a monitoring system can help to the detection and report of any unusual or suspect activities within the system. This system can monitor the network traffic, the users' activities, the events from the system and other security relevant activities. In case of detection of any suspect activities, the system can generate alerts in order to notify the security managers in order to take the necessary measures.

The number of natural data subjects affected by the incident is of **24**.

Under section "Possible consequences and adverse effects (risks) for the natural data subjects" from the security breach notification form submitted by **Hyllan Pharma SRL** it is mentioned that "the financial frauds (Lei 400) will be recovered with the help of the bank".

Also, within the same notification form, under section "Technical and organisational measures taken by the controller in order to mitigate the eventual negative effects", the following are mentioned:

1. The controller acknowledged in a short period of time the incident and ordered measures in order to handle it.
2. The data protection officer was contacted in order to bring to the knowledge and manage this risk.
3. The incident response team/commission met in the shortest possible time (11.01.2023) and analysed all relevant aspects, the priorities and steps to be further followed were established.
4. The reset of the vps access password was requested.
5. Within the ticket howx-9242-hjei the activation of the two-factor authentication was requested, that was performed on 10.01.2023 time 15:10.
6. The access passwords for all domains (passwords that were changed several weeks before, different for each domain and random generated) were changed.

It is mentioned that the information of all natural data subjects was performed, both by phone and by e-mail.

II. Handling proceedings performed by ANSPDCP

Through the letter no. 3770/23.02.2023, ANSPDCP requested additional information from **Hyllan Pharma SRL,** which responded through the letters no. 4532/07.03.2023 and no. 4557/07.03.2023 as it follows:

Q1: "the manner of manifestation of the cyberattack"

R1: *The cyberattack manifested as it follows: when placing an order, at the moment when the client chose as payment method – bank card and should have been redirected to the Netopia payment processor, he was actually redirected through an intermediary screen generated by the index.php file from the CC folder.*

In order for this redirection to the intermediary page to be performed, the hacker managed to amend also the page Netopia.php that contained the redirection to ***https://secure.mobilpay.ro/*** *in the sense that it changed the code so as the client to get on the phishing page "**public_html/CC/index.php**".*

Also, the cyber attack was type PHP injection, that is a form of cyberattack when an attacker uses a vulnerability within a web application ruling the PHP in order to execute their malicious code within the application. This can lead to the compromise of the data, to obtaining the unauthorized access to the resources of the application or to its complete take-over.

The PHP Injection type cyberattack manifested through the code injection: the attacker can insert a malicious code within a form or web interface running PHP. This code can be used in order to obtain access to the database of the application, in order to manage the data or to launch other attacks.

Q2: "the effects of the cyberattack on the hardware and software infrastructure, as well as on the electronic communication resources/channels used";

R2: *The effects of a PHP Injection type cyberattack can lead to the loss or compromise of the data, of the confidentiality, integrity or availability of the web application.*

Compromise of the data: The attacker can obtain access to the sensitive data, such as personal information, authentication details, financial information or other confidential information. This information can be used in unfavourable ways, such as fraud or identity theft.

Following the cyberattack **no effects** on the hardware and software infrastructure, as well as on the electronic communication resources/channels used by SC HYLLAN PHARMA SRL **were registered**. The breach was closed, and at this moment everything is functioning normally, without damages.

From a financial perspective, an unauthorized payment on behalf of a single data subject was performed. The blocking of the payment through bank was obtained and the money sum was fully recovered.

Q3: "the system logs on the access and/or download of the files/databases that are subject to this incident, with the mention of they were accessed and/or downloaded":

R3: We hereby provide you these system logs within the attachment (Annex 1).

Ip: 196.117.25.146

Q4: "the total number of natural data subjects affected by the security incident"*:*

R4: 25 natural data subjects

Q5: "the content of the information for the natural data subjects affected by the security incident"

R5: We provide you the **Information letter** for the data subjects affected by the security incident within the attachment (Annex 2).

Q6: "the investigation report for the notified security incident, if there was an internal investigation or with experts within the domain":

R6: We hereby provide you the official request for the investigation of the phishing incident provided (on 10.01.2023) by Hyllan Pharma SRL to the service provider ROMARG SRL in attachment (Annex 3).

Q7: " Considering those stated under point 16 from the notification form, namely the fact that also natural persons from other Member States were affected, we hereby request you to mention broken down by each Member State of the European Union the number of natural data subjects affected"

R7: Romania: 21 data subjects affected.

Italy: 4 data subjects affected

Q8: "Considering the provisions of Article 24 and Recitals 75 and 76 from the Regulation (EU) 2016/679, with reference to point 11 from the notification, "eventual adverse consequences and effects (risks) for the natural data subjects", **we hereby request you to provide us if there is any evaluation procedure/methodology for the risk on the persons' rights and freedoms**"

R8: We hereby provide you in attachment (Annex 4-The evaluation of the risk corresponding to the incident for the personal data security), within **point II** – the identification of the risk factors and **point III**- the risks' matrix, the procedure/methodology for the evaluation of the risk on the persons' rights and freedoms in the case of that incident.

The following technical measures were taken:

- The access data of the users managing the pages were changed
- The two-steps authentication with password available for two minutes was implemented
- We constantly follow the authentication log, to see if authentications at unusual hours appear
- We created a soft that monitors the status of the system by verifying two consecutive statuses so, if there are extra files or files are erased or the dimension of a file is amended, we have the alert on e-mail

Q9: "Considering the provisions of Article 24 and Recitals 75 and 76 of Regulation (EU) 2016/679, by reference to point 11 from the notification "eventual consequences and adverse effects (risks) for the natural data subjects", **we request you to provide us with an evaluation regarding the risk for the persons' rights and freedoms, that would encompass inclusively the fitting into a risk degree (low, medium, high)**

R9: We provide you attached (Annex 4) the **Assessment of the risk** corresponding to the incident for the personal data security (performed on 12.01.2023)

Q10: "The service agreement concluded by **HYLLAN PHARMA SRL** with the processor **ROMARG SRL**"

R10: We hereby provide you attached the Service agreement concluded by HYLLAN PHARMA SRL with the processor ROMARG SRL (Annex 5).

III. Information of the concerned supervisory authorities within IMI

On 27.09.2023, through the IMI application, the other supervisory authorities were informed (specifically the authority from Italy), within a LSA and CSA identification procedure regarding the security incident (based on Article 56 of the GDPR), as well as in relation to the intention of our institution to act as lead supervisory authority, registered under no. 561108, with response deadline until 29.12.2023.

Until the date of this decision, the following supervisory authorities declared themselves as CSA:

- The supervisory authority from Italy;
- The supervisory authority from Spain (with the mention: "according to the information available, there are no sufficient elements to ensure that the data subjects from Spain have been affected, so ES SA is not CSA. However, in case additional proofs according to which the natural data subjects from Spain are affected are identified, ES SA would be CSA)";

On 15.04.2024, the Italian supervisory authority was informed, through the IMI application, about the draft Decision, without making observations/comments on the ANSPDCP proposal.

IV. Conclusions:

From the investigation performed by ANSPDCPD through letters no. 3770/23.02.2023 and from the responses of **Hyllan Pharma SRL** no. 4532/07.03.2023 and no. 4557/07.03.2023, the following resulted:

- within 06.01.2023 – 10.01.2023 an illegal/unauthorized access to the personal data of a number of 24 natural data subjects (clients) of Hyllan Pharma SRL, that acquired online products through 4 websites (profecund.it, profecund.ro, normens.ro, steablock.ro) was found. The infrastructure for the storage of the data is managed by the processor "Romarg SRL";
- a hacker accessed unauthorized the database of Hyllan Pharma, by adding an information structure within a file that was collecting the card data of the data subjects;
- the collection was performed by the hacker by creating a fraudulent page that was redirecting to Netopia the data on one hand, but also to the e-mail address ahmadgeniius@outlook.com;
- the possibly compromised personal data, in the sense that the attacker could obtain access to personal information, authentication details, financial information or other confidential information are: first name, last name, address, city, country, email, credit card number, name from the credit card, expiry date and CVC;
- the number of affected persons is of 24 natural data subjects;
- the cyberattack was a malware attack type "**php.malware.fopo**", being a form of malware that is injected within the web applications written in PHP.
- as immediate effects of a PHP.Malware.FOPO (PHP Object Injection) attack may vary depending on the purpose and abilities of the attacker, but may include: unauthorized access to the application's data, information theft, distribution of additional malware;
- as technical and organisational measures were applied by the controller, both before and after the incident, the following:
  a) the ordering of measures for the handling of the attack;
  b) the contacting of the Data Protection Officer;
  c) the reunion of the incidents' response team/commission in the shortest time and there have been analysed the relevant aspects and the establishment of the priorities and steps to be followed;
  d) the reset of the VPS access password;
  e) the activation of Two-Factor-Authentication;
  f) the change of all access passwords for all web domains (passwords that were changed with several weeks before, different for each domain and randomly generated).

g) The opening of a criminal action from the perspective of committing the crime of illegal access to data provided under Article 360 paragraph (3) from the Criminal Code corroborated with Article 364 – Illegal transfer of data;
h) The notification of the National Cyber Security Directorate in order to support the research and to offer the recommendations necessary for the reduction of the risks corresponding to the incident;
i) The creation of a software that monitors the status of the system by verifying two consecutive statuses so as if there are extra files or files are erased or the dimension of a file is amended to provide an alarm on the e-mail.

V. Analysis according to the criteria provided under Article 83 GDPR

The conclusions resulting following the analysis of the security incident according to the criteria from Article 83 of the GDPR:

a) the nature, gravity and duration of the infringement, the scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them:
- 25 data subjects (24 clients and 1 employee)
- The systems of Hyllan Pharma SRL were subject to a PHP Injection cyberattack following which the hacker modified the Netopia.php page that contained the redirection to https://secure.mobilpay.ro/ in the sense that it changed the code so as the client to get on the phising page ”public_html/CC/index.php” when he was choosing the payment method – credit card;
- No complaints were submitted by the data subjects affected by the security incident notified by Hyllan Pharma SRL, therefore no damages incurred by the latter were able to be identified

b) the intentional or negligent character of the infringement
- ”php.malware.fopo” malware cyberattack

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the data subjects affected by the incident were informed through the electronic mail (email) inclusively in relation to the security of the credit cards in order to avoid potential damages
- the transactions were blocked and the financial frauds were recovered (Lei 400, the equivalent of Eur 800);
- an evaluation on the risk for the rights and freedoms of the data subjects was performed;
- after the incident took place additional technical and organisational measures were taken.

d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
- immediately ordered measures for handling the attack;
- summoned the incident response team/commission in the shortest time and analyzed the relevant aspects and established the priorities and steps to be followed;
d) resetting the VPS access password;
e) the activation of Two-Factor-Authentication;
f) the change of all access passwords for all web domains (passwords that were changed with several weeks before, different for each domain and generated randomly)
g) the opening of a criminal action for the crime of illegal access to data provided under Article 360 paragraph (3) from the Criminal Code corroborated with art. 364 Illegal transfer of data;
h) the notification of the National Directorate for Cyber-Security in order to support the research and offer the necessary recommendations for the reduction of the risks corresponding to the incident;
i) the creation of a soft that monitors the status of the system by verifying two consecutive statuses so if additional files appear or files are deleted or the size of a file is changed to submit an alarm on e-mail.

e) any relevant previous infringements by the controller or processor;

- no previous breaches were identified

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement:

- the controller **notified the security incident within the deadline provided under the GDPR and communicated to ANSPDCP all information requested within the investigation performed;**

g) the categories of personal data affected by the infringement:

- first name, last name, city, country, email, credit card number, name from the credit card, expiry date and CVC;
- according to the system's logs regarding the access and/or download of the files/databases it resulted that **the personal data have not been downloaded or accessed**;

h) the manner in which the infringement was brough to the knowledge of the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement:

- the controller **notified the security incident within the deadline provided under the GDPR and communicated to ANSPDCP all the information requested within the investigation performed**

i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures:

- no measures were previously applied

j) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement:

- the security incident took place following a malware cyberattack

Considering the conclusions resulting from the investigation performed at Hyllan Pharma SRL, the technical and organisational measures taken by the controller, the fact that the data subjects affected were informed through electronic letter, as well as the fact that from the verification of the ANSPDCP's registrations, it resulted that based on the GDPR there have not been applied sanctions against Hyllan Pharma SRL, we consider that the measures adopted by the controller in the sense of Article 34 paragraph (3) letter b) of the GDPR are sufficient, which is why **we consider that in this case the application of a sanction is not required**.

President,

Ancuța Gianina OPRE