Procedure No:PS/00059/2019

FINAL DECISION ON PENALTY PROCEEDINGS

Of the proceedings conducted by the Spanish Data Protection Agency and based on the following

BACKGROUND

FIRST:On29/06/2018, TYPEFORM S.L. (hereinafter TYPEFORM) notified the Agency of a safety gap in which it reports unauthorized access (cyber-attack) to databases hosted in AMAZON AWS (Amazon Cloud).

On 27/07/2018, TYPEFORM notified the Agency of a second security gap, due to access to the databases hosted in AMAZON AWS, with three stolen credentials and data mining.

According to the information they provide, EU countries may be affected in both gaps.

The notifications of security gaps reveal a possible breach of the rules on the protection of personal data. The data processing carried out may have affected data subjects in several Member States. For this reason, through the *'Internal Market Information System'* (hereinafter 'IMI'), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), which aims to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information, the Agency transferred the facts to the other supervisory authorities. The transfer of these facts received by the AEPD is carried out in accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter GDPR), taking into account their cross-border nature. This Agency is competent to act as lead supervisory authority.

According to the information incorporated into IMI, pursuant to Article 60 GDPR, the supervisory authorities in Germany (Thuringia, North Rhine-Westphalia, Hesse, Mecklenburg-Western Pomerania, Lower Saxony, Bavaria and Saarland), Austria, Denmark and Romania have been identified as interested in the present proceedings.

SECOND: IN the light of the facts and documents brought to the knowledge of this Agency, the Subdirectorate-General for Data Inspection carried out preliminary investigations to clarify the facts in question, in accordance with the powers of investigation conferred on the supervisory authorities in Article 57 (1) of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), and in accordance with the provisions of Title VII, Chapter I, Section II of Organic Law 3/2018 of 5 December on the Protection of Personal Data (DGDD), and in accordance with the provisions of Title VII, Chapter I, Section II of Organic Law of on the protection of digital data.

As a result of the investigations carried out, we are aware of the following:

TYPEFORM is a company owning a WEB based platform that allows the creation from surveys to IT applications, without the need for IT development skills, designed for use by end users (Typeformers).

TYPEFORM has submitted to this agency the following information concerning the safety gaps reported to the Agency:

Description and timeline of the first safety gap notified to the AGPD on 29/06/2018:

1.On 27/06/2018, at 13: 30, an alert was generated by the monitoring systems (*Amazon AWS*GuardDuty) in the cloud environments (Amazon AWS) and reviewed by the company's security staff. The company contracts the AMAZON AWS Guard Duty service in March 2018 as a result of the adaptation to the new data protection rules.

"Amazon Web Services (AWS) is a secure cloud service platform that provides computational power, database storage, content delivery and other functionalities for businesses". "Amazon GuardDuty is a threat detection service that monitors continuously to detect malicious or unauthorized behavior and help you protect your AWS workloads and accounts. Monitor activities such as unusual API calls or potentially unauthorized implementations that may indicate a potential danger to the account.GuardDuty also detects potentially vulnerable actors or reconnaissance activities by attackers."

The investigation carried out by the security and operations teams confirms the safety gap from an unidentified attacker. Access logs to AMAZON's APIs indicate that an access key has been used for unauthorized access to company files located in Amazon's cloud to extract information.

'An API is a set of instructions and procedures (software) that perform predetermined functions, which can be used by other software. API stands for Application Programming Interface. An API access key would make it possible to invoke certain APIs that the cloud owner makes available to its customers in order to facilitate their IT development."

At 13: 35, this access key is revoked and public access to the server is restricted, only accessible from the company's private network. The attacker's IP address is also blocked at network level.

During the rest of the day, the information that has been affected has been deleted and your consultant is contacted in order to obtain information on the management of the safety gap and to make the appropriate notifications.

2.On 28/06/2018 outgoing communications were restricted and a new server was launched where only uncompromised configuration information was copied. On the same date, he sent them the interim report on the results of the analysis of the safety gap, a copy of which is attached.

3.On 29/06/2018, all production credentials (information system accessed by users) that include databases and user account access keys are changed.

All tokens are also revoked and renewed to company applications that have been committed to the gap and permits are eliminated for all users except operational and security equipment.

"An access token is a random password (character string) that identifies a user and can be used by the application to make API calls."

As the attacker might have had access to data from the forms used by the company's users that might contain personal data, communication is sent to the users affected by the security incident. They provide a copy of the communication sent.

4.On 30/06/2018, the security team concludes the examination of ports and IP addresses with public access to the production environment and closes access that is not strictly necessary.

5.On 06/07/2018, the consultant submitted the final report on the results of its analysis of the safety gap, a copy of which was provided. On 12/07/2018 the corresponding complaint was lodged with the Guardia Civil (Technical Investigation Team of the Criminal Police of the Civil Guard in Barcelona).

As regards the causes that made the cyber-attack possible, according to the report issued by implication, [redacted]

[redacted]

Description and timing of the second safety gap reported to the AEPD on 27/07/2018:

1.25/07/2018 at 16: 40, an alert is generated by the monitoring systems (Amazon AWS GuardDuty) in the cloud environments (Amazon AWS) and reviewed by the company's security staff.

The investigation carried out by the security and operations teams confirms the safety gap from an unidentified attacker. Access logs indicate that an access key has been used for unauthorized access to Amazon cloud file systems to extract information.

At 16: 40, the three access keys affected by the incident are revoked and network attacking IP addresses are also blocked.

At 17: 30, the consultant was contacted in order to obtain information on the management of the safety gap and to make the appropriate notifications.

At 19: 00, the security team restricts access to two company files containing Amazon AWS access keys and leaves only access to the operations team. Similarly, general access is also restricted for all non-essential employees in the company.

At 20: 20, security equipment strengthens the use of 'multi-authentication factor' for all users.

At 22: 00, only access to the IPIs of the AWS office and local network is allowed.

2.On 26/07/2018, it is identified that the access keys of two employees are being used from a suspicious location, thus changing all passwords of these users.
3.On 27/07/2018, a new Amazon AWS account is created and all non-trading employees are moved to the new account so that they can conduct tests, setting access according to different profiles (roles).

4.On 06/08/2018, the consultant submitted the final report on the results of its analysis of the security gap, a copy of which was submitted and on 22 August the corresponding complaint was lodged with the Guardia Civil (Technical Investigation Team of the Judicial Police of the Civil Guard in Barcelona).

With regard to the causes that have made the cyber-attack possible: [redacted] Despite some similarities between the two attacks, none of them has led to the conclusion that there is a link between the two attacks.

In relation to the number of persons affected by the incidents, the typology of the data and the nationalities of the data and the companies of which they are clients:

1.In the first security gap, the number of account holders 'Typeformers' (customers of the company) affected is 232.766, although they are not aware of their nationality, since this is not requested in the process of registering users, if you have information on the place of residence of the users. Please find attached a list of the countries of residence and the number of users in each country. The list includes more than 170 countries, including almost all countries in the European Union.

As regards the 'respondents' concerned (persons completing the surveys or forms created by the Typeformers), they do not have any data since the content of the surveys is defined individually by the Typeformers and it is they who decide whether to request personal data and their typology, without the company controlling or accessing that information.

TYPEFORM made a communication model available to clients (Typeformers) so that they could inform respondents.

The data that the attacker was able to access for Typeformers are username and e-mail address and for respondents, the data contained in the forms or surveys (these data vary according to the Typeformer).

2.In the second security gap, the number of account holders (Typeformers) affected is 2.892.786, although the number is higher than in the first, the attacker was only able to access Typeformers' username and mail address data, not having access to the content of the forms or surveys or, consequently, to respondents' data. Please find attached a list of the countries of residence and the number of users in each country. The list includes more than 170 countries, including almost all countries in the European Union.

With regard to the measures taken by the undertaking in relation to the security gaps: In addition to those indicated in the chronological description, the following corrective actions have been implemented:

On 03/10/2018, logs for authentication of production machines began to be registered in the monitoring and alert system.

— On 15/10/2018, several production services were moved in order to be able to obtain centralized authentication.

— On 25/10/2018, it is the start date of the scans on their websites in search of vulnerabilities, which are carried out on a regular basis to alert them to any potential vulnerability that may arise in production. To this end, the services of two world-leading companies have been contracted.

— On 05/11/2018, safety training courses were completed for all employees of the company, which were organized because of the security gaps. They provide a copy of the presentation used in these courses.
They note that all employees had already received the relevant training prior to 25 May 2018 as part of the GDPR compliance process. They provide copies of the presentations used in these courses from March to May.

On the use by third parties of data obtained through cyber-attacks

1.The company is not aware that these data have been used by third parties. they have consulted both the incident and the CERT for Security and Industry (Ministry of Energy, Tourism and the Digital Agenda), as well as with the staff of the Guardia Civil's Technology Research Team and all of them have confirmed that, given the typology of the attacks, it is not easy to obtain such information.

2.The staff of the Guardia Civil have confirmed that they are making letters rogatory to other countries, but that no results will be obtained in the short term.

THIRD: In accordance with the powers conferred on it by the GDPR, the Spanish Data Protection Agency would be competent to adopt decisions designed to produce legal effects, be it the imposition of measures to ensure compliance with the rules or the imposition of administrative fines. However, it is obliged to closely involve and coordinate the supervisory authorities concerned in the decision-making process and to take their opinion into account to the greatest extent. It also provides that the binding decision to be adopted is to be agreed jointly.

Article 60 GDPR regulates this cooperation between the lead supervisory authority and the other supervisory authorities concerned. Paragraph 3 of that article expressly provides that the lead supervisory authority is to forward to the other supervisory authorities concerned, without delay, a draft decision in order to obtain its opinion on the matter and shall take due account of its views, in accordance with the procedure laid down in paragraph 4 et seethe supervisory authorities concerned have a period of four weeks to raise reasoned objections to the draft decision, it being understood that there is agreement on the draft decision if no objection is raised by any authority within the prescribed period, in which case all of them are bound by the repeated draft.

Article 60(12) provides that the lead supervisory authority and the other supervisory authorities concerned shall provide each other with the information required under this

Article by electronic means. This should be done through the "Internal Market Information System" (IMI).

Moreover, Article 58 (4) GDPR provides that the exercise of the powers conferred on the supervisory authority must respect the procedural safeguards laid down in Union and Member State law.

It therefore considered it appropriate and appropriate for this Agency to adopt a draft agreement to initiate penalty proceedings at the time of the notification referred to above and to submit it to the authorities concerned, as listed above, so that they can raise any objections they consider relevant or agree to the present opening plan.

The adoption of this draft agreement to initiate penalty proceedings is provided for in Article 64 of the LOPDGDD, paragraphs 2 (third paragraph) and 3, providing for the obligation to give formal notice to the person concerned, according to which such notification shall interrupt the limitation period for the infringement.

Furthermore, Article 64 (4) of the LOPDGDD provides that the processing time limits laid down in this Article shall be automatically suspended when information, consultation, request for assistance or a mandatory decision must be obtained from a body or body of the European Union or from one or more supervisory authorities of the Member States in accordance with the GDPR, for the time between the request and the notification of the decision to the Spanish Data Protection Agency.

Once any comments from the supervisory authorities concerned have been analyzed, the required agreement to initiate penalty proceedings shall be adopted, if appropriate, which shall be notified to the person or entity against whom the penalty is addressed.

In accordance with the procedure laid down in Article 60 of the GDPR, on 01/04/2020 the Director of the Spanish Data Protection Agency agreed to adopt a draft agreement to initiate penalty proceedings against TYPEFORM S.L. and in accordance with the procedure laid down in Article 60 GDPR, the draft decision to initiate proceedings was transmitted via the IMI system to the supervisory authorities concerned and informed them that if they did not object within four weeks of the consultation, the draft decision to initiate proceedings was transmitted through the IMI system to the supervisory authorities concerned and to inform them that, if they did not object within four weeks of the consultation, the mandatory infringement agreement would be adopted.

FOURTH: After the draft opening of proceedings was submitted to the supervisory authorities concerned in accordance with Article 60 (3) GDPR, the following objections were raised in summary within the prescribed legal deadline:

France

The French Authority points out that the draft agreement does not set out the legal reasoning for classifying the company's alleged infringements; it points out that the facts explain the context of the data breach, but do not explain the constitution and characterization of the alleged violations committed by TYPEFORM which its authority proposes to penalize.

Holland

The Dutch Authority expresses, like the previous one, that even though the AEPD rightly concludes that Articles 32, 33 and 34 GDPR are not complied with, it requires a general description of the legal reasoning to be included in the draft decision supporting the

conclusion of sanctioning those infringements. Currently, only a chronology of the events is included, but no legal assessment of these facts is included.

Regarding the alleged breach of Article 32 GDPR, we note that an assessment of whether the technical and organizational measures that the company had implemented at the time of the incidents were in fact appropriate for the risk profile of the company and its data processing.

Norway

The Norwegian Authority notes that the decision contains the facts, legal grounds, and conclusion; it would be useful for both the authorities and the addressees of the decision to see the reasoning behind the decision.

Hungary

The Hungarian Authority notes that the project does not contain any relevant information other than the circumstances of the hacker attack, the measures taken by the controller and the sanction to be imposed; however, it does not include the finding of the infringement or the legal reasoning.

Denmark

Like the other authorities, it points out that more information would be needed.

The objections were received and were then answered that: in relation to the type of document shared through IMI, this is a draft agreement to initiate penalty proceedings and that, according to the Spanish rules on administrative procedure, the decision to initiate the procedure must contain succinctly the facts, the person responsible for them, the alleged infringement that may have been committed and the amount of the fine to be imposed. Throughout the procedure, all information and actions must be completed.

As regards the reasons for proposing the initiation of a penalty procedure, it was found that, following the analysis of the security measures implemented by the company responsible before suffering the two security gaps, it was found that they were not sufficient and adequate to prevent the attacks suffered. Since this is confidential information of the company, it is usually not collected in the penalty proceedings and, in Spain, decisions are published once signed by the Director of the Agency.

The amount of the penalty is calculated considering these circumstances:

The international and non-local extent of the declared safety gap,

The link between the offender's activity and the processing of personal data.

The degree of responsibility of the controller, considering the technical or organizational measures implemented.

There is no evidence that the entity acted intentionally.

The way the supervisory authority became aware of the infringement.

The degree of cooperation with the supervisory authority.

— There is no record of a previous infringement committed by the person responsible.

FIFTH: On 18/02/2021, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against the complainant, in accordance with Articles 63 and 64 of Law 39/2015 of 1 October on the Common Administrative Procedure of Public

Administrations (LPACAP), for the alleged infringement of Article 32 (1) of the GDPR, as defined in Article 83 (4) (a) of the GDPR.

SIXTH: TYPEFORM has acknowledged its responsibility for the events revealed in the reported security incidents.

FACTS

FIRST: TYPEFORM is a company owning a WEB based platform that allows the creation from surveys to IT applications, without the need for IT development skills, designed for use by end users (Typeformers).

SECOND: On27/06/2018, at 13: 30, an alert was generated by the monitoring systems (*Amazon AWS*GuardDuty) in the cloud environments (Amazon AWS) and reviewed by the company's security staff. On 29/06/2018, TYPEFORM notified the Agency of a safety gap reporting unauthorised access (cyber-attack) to databases hosted in AMAZON AWS (Amazon Cloud).(the actions carried out by Typeform are explained in detail in the second paragraph).

THIRD: On 25/07/2018 at 16: 40, an alert is generated by the monitoring systems (Amazon AWS GuardDuty) in the cloud environments (Amazon AWS) and reviewed by the company's security staff.

The investigation carried out by the security and operations teams confirms the safety gap from an unidentified attacker.
On 27/07/2018, TYPEFORM notified the Agency of a second security gap, due to access to the databases hosted in AMAZON AWS, with three stolen credentials and data mining. (the actions carried out by Typeform are explained in detail in the second paragraph).

FOURTH: According to the information they provide, EU countries may be affected in both gaps.

FIFTH: On the use by third parties of data obtained through cyber-attacks

- The company is not aware that these data have been used by third parties. they have consulted both the incident and the CERT for Security and Industry (Ministry of Energy, Tourism and the Digital Agenda), as well as with the staff of the Guardia Civil's Technology Research Team and all of them have confirmed that, given the typology of the attacks, it is not easy to obtain such information.

GROUNDS

I

Under the powers conferred on each supervisory authority by Article 58 (2) of the GDPR, and as laid down in Articles 47, 48, 64.2 and 68.1 of the LOPDGDD, the Director of the Spanish Data Protection Agency is competent to resolve this procedure.

Article 63 (2) of the LOPDGDD provides that: *'The procedures conducted by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, in this Organic Law, by the regulatory provisions adopted in its implementation and, in so far as they do not contradict them, in the alternative by the general rules on administrative procedures.'*

II.

Article 56 (1) GDPR, concerning *the 'Competence of the lead supervisory authority*', provides:

'1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60."

Article 60 governs *'Cooperation between the lead supervisory authority and the other supervisory authorities concerned*':

'1.The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavor to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2.The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3.The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

4.Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.

5.Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.

6.Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.

7.The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority to which a complaint has been lodged shall inform the complainant on the decision.

(...)

12.The lead supervisory authority and the other supervisory authorities concerned shall provide each other with the information required under this Article by electronic means using a

standard form."

On the issues covered by these provisions, account is taken of recitals 124, 125, 126 and 130 of the GDPR.

In accordance with the above rules, in the present case, which concerns, inter alia, the communication of two security gaps in the context of the activities of a single establishment of a controller substantially affecting data subjects in more than one Member State (cross-border data processing), the lead supervisory authority, in this case the Spanish Data Protection Agency, is obliged to cooperate with the other authorities concerned.

The Spanish Data Protection Agency, in application of the powers conferred on it by the GDPR, is competent to adopt decisions designed to produce legal effects, whether the imposition of measures to ensure compliance with the rules or the imposition of administrative fines. However, it is obliged to closely involve and coordinate the supervisory authorities concerned in the decision-making process and to take their opinion into account to the greatest extent. It also provides that the binding decision to be adopted is to be agreed jointly.

Article 60 GDPR regulates this cooperation between the lead supervisory authority and the other supervisory authorities concerned. Paragraph 3 of that article expressly provides that the lead supervisory authority is to forward to the other supervisory authorities concerned, without delay, a draft decision in order to obtain its opinion on the matter and shall take due account of its views, in accordance with the procedure laid down in paragraph 4 et seethe supervisory authorities concerned have a period of four weeks to raise reasoned objections to the draft decision, it being understood that there is agreement on the draft decision if no objection is raised by any authority within the prescribed period, in which case all of them are bound by the repeated draft.

Article 60(12) provides that the lead supervisory authority and the other supervisory authorities concerned shall provide each other with the information required under this Article by electronic means. This should be done through the "Internal Market Information System" (IMI).

Moreover, Article 58 (4) GDPR provides that the exercise of the powers conferred on the supervisory authority must respect the procedural safeguards laid down in Union and Member State law.

Spanish procedural rules, in particular Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), provide that penalty proceedings must always be initiated ex officio by agreement of the competent body, which must include, inter alia, the identification of the person (s) suspected of being responsible, the facts justifying the initiation of the procedure, their possible classification and any penalties that may be applicable.

In accordance with the rules set out above, in view of the cross-border nature of this complaint, a draft agreement to initiate penalty proceedings was issued, which was subsequently transmitted via the IMI system to the supervisory authorities concerned, which are referred to in the background, and it is therefore understood that there was

agreement on it.

For the same reasons and for the same purpose, the decision which decides and closes the present proceedings must also be communicated to the supervisory authorities concerned with the submission of the draft decision on the penalty proceedings.

Furthermore, Article 64 (4) of the LOPDGDD provides that the processing time limits laid down in this Article shall be automatically suspended when information, consultation, request for assistance or a mandatory decision must be obtained from a body or body of the European Union or from one or more supervisory authorities of the Member States in accordance with the GDPR, for the time between the request and the notification of the decision to the Spanish Data Protection Agency.

Once any comments from the supervisory authorities concerned have been analyzed, the necessary decision on the penalty procedure shall be adopted, if appropriate, which shall be notified to the person or entity against whom the penalty is addressed.

III.

The present proceedings were initiated by the communication of two security gaps. The security of personal data is regulated in Articles 32, 33 and 34 GDPR.

The facts reported by the company refer to the existence of two security incidents (gaps) in June and July 2018 informing the AEPD of unauthorized access to the databases hosted in Amazon's cloud, affecting a very large number of users and located in a large number of countries, including the majority of the European Union.

These facts could constitute an infringement of Article *32 GDPR 'Security of processing'*, which provides:

'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 risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) pseudonymization and encryption of personal data;
(b) the ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data rapidly in the event of a physical or technical incident;
(d) a process of regular verification, evaluation and assessment of the effectiveness of technical and organizational measures to ensure the security of 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, unauthorized 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 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4.The controller and the processor shall take measures to ensure that any person acting under the authority of the controller or the processor and having access to personal data may process such data only on instructions from the controller, unless required to do so by Union or Member State law."

Recital (83) states that:

"(83) In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should assess the risks inherent in the processing and implement measures to mitigate them, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. When assessing the risk in relation to data security, account should be taken of the risks arising from the processing of personal data, such as the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or unauthorized disclosure of, or access to, such data, which could in particular result in physical, material or non-material damage."

The actions carried out and the documentation submitted to the file show that the security measures implemented by the entity under investigation in relation to the data that was being processed were not the most appropriate to guarantee the security and confidentiality of personal data at the time of the security incidents.

As also stated in recital 39:

"... Personal data should be processed in a way that ensures adequate security and confidentiality of personal data, including to prevent unauthorized access to or use of such data and of the equipment used for the processing".

It should be noted that security measures are key to ensuring the fundamental right to data protection as this fundamental right cannot be guaranteed if the confidentiality, integrity and availability of personal data cannot be guaranteed. Both technical and organizational measures are necessary to ensure these three safety factors.

It should be noted that in the present case, in the light of both the forensic company's report and the entity's own statements, serious vulnerabilities in the respondent's systems are apparent, compromising the confidentiality and integrity of the security of the information by causing unauthorized access and unlawful transmission of data as a result of the two security gaps declared and notified by the respondent.

Both the first and second gaps reported by the respondent confirm that they are caused by unidentified attackers and that access logs (files) to AMAZON's APIs indicate that an access key has been used for unauthorized access to company files located in Amazon's cloud to extract information.

Firstly, it should be noted that the complainant did not have an impact assessment because the data processing was old and dedicated to implementing security measures according to the convenience and state of the technology.

Secondly, it is apparent from the report that, on 27/06/2018, alerts from Amazon Web Services*' Guard Duty* system were reviewed when the system itself detects attempts to attack Amazon Web Services or irregular access.

The actions carried out through the committed key were to list various resources in the Amazon Web Services environment of Typeform, as well as its instances, databases and data storage spaces in S3, to locate backup copies stored in these storage spaces and finally to download them.

The key was used in an instance of Amazon Web Services hosting a service known as Jenkins. This service is used internally by the company for its software and system development operations, however, it was accessible from the public network.

The prior action report itself states that:

As *regards the causes that made the cyber-attack possible, according to the report issued by implication,* [redacted]

And that, in the second divide, the attacker [redacted] and, moreover, none of the IPs used *in the first attack were used in the second and despite certain similarities between the two attacks, none of them has led to the conclusion that there is a link between the two attacks.*

Following the investigations, it was established that:

The service displayed, known as [redacted] was an old version of the service.

On the machine hosting the [redacted] service, it is determined that the committed API key is located in one of the configuration files living on the machine. This key is loaded into the [redacted] application as an environment variable. It further noted that "*t*[redacted]

Clear signs of automated attacks were found on the machine where the service is hosted. On that machine, it can also be observed that there has been a high volume of web traffic compared with the previous log rotation, even though it is more than one year old.

The consequences of the first security gap are that the number of clients of the company (Typeformers)affected is 232.766, and although their nationality is not known, the place of residence of those affected is more than 170 countries, including almost all those in the European Union.

With regard to the *'respondents'* concerned (persons completing the surveys or forms created by the *Typeform*ers), they do not have data since the content of the surveys is defined individually by the Typeformers and *it is they who decide whether or not to request personal data and their typology, without the company controlling or accessing that information.*

And for the data to which the attacker was able to access for Typeformers, *there* are the username, e-mail address and, for the respondents, the data contained in the forms or surveys.

As regards the second security gap, the number of customers of the company affected was much higher, 2.892.786, although the attacker was only able to access Typeformers' username and mail address data and could not access the content of the forms or surveys or, consequently, the respondents' data.

Therefore, in the light of the above paragraphs, it follows that, given the technological evolution of personal data processing activities, they must be addressed from the point of view of continuous risk management, by defining the control and security measures that are necessary to ensure that the processing takes place in compliance with the privacy and confidentiality of the data and by regularly and continuously assessing the effectiveness of the control measures put in place.

This also implies the protection of personal data by design and by default, i.e. that the controller applies, both when establishing the means of processing and at the time of processing, all appropriate technical and organizational measures designed to effectively implement data protection principles, and to integrate, in the processing, the necessary safeguards to comply with the requirements of the GDPR; in addition, the controller should implement those measures to ensure that, by default, only the personal data necessary for each specific purpose of the processing are processed.

That mere possibility of access to data poses a risk which must be analyzed and assessed when processing personal data and which increases the level of protection regarding security and safeguards the integrity and confidentiality of the data.

This risk should be considered by and based on the controller to establish appropriate measures that might have prevented the loss of control over the data and thus their access to the respondent's systems as demonstrated.

The description of the deficiencies found in the security measures implemented by the requested person prior to suffering from the notified security gaps, which were to a large extent the reason for the occurrence of those incidents, amounts to a breach of Article 32 (1) GDPR, as defined in Article 83 (4) (a) of the GDPR.

Article33 GDPR provides that, in the case of a personal data breach, the controller shall

notify the personal data breach to the competent supervisory authority in accordance with Article 55 without undue delay and, if possible, no later than 72 hours after having become aware of it, unless the security breach is unlikely to constitute a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

In the present case, Typeform notified the two security gaps within the deadline set out in the GDPR, with the information set out in the same article.

Article 34 GDPR indicates that where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. Following the study carried out by the person responsible for the gaps, as with the CERT for Security and Industry (Ministry of Energy, Tourism and the Digital Agenda), as well as with the staff of the Guardia Civil's Technology Research Team, all confirmed that, given the typology of attacks, it is not easy to obtain such information; as a result, there is no high risk to the rights and freedoms of natural persons which would require the persons concerned to be informed.

IV

Article 83 (4) (a) GDPR considers that the infringement *of "the obligations of the controller and processor under Articles 8, 11, 25 to 39, 42 and 43*" is punishable, according to Article 83 (4) of the GDPR, "with administrative fines up to EUR 10 000 000 or, in the case of an undertaking, up to 2 % of the total overall annual turnover of the preceding financial year, whichever is the higher."

Article 71 of the LOPDGDD, Infringements, states that: *'The acts and conduct referred to in Article 83 (4), (5) and (6) of Regulation (EU) 2016/679 and those contrary to this Organic Law shall constitute infringements.'*

Article 73*, Infringements considered to be* serious, provides that:

'In accordance with Article 83 (4) of Regulation (EU) 2016/679, infringements which constitute a substantial infringement of the articles referred to therein, and in particular the following, shall be regarded as serious and shall be time-barred after two years:

(...)
(g) breach, as a result of the lack of due diligence, of the technical and organizational measures put in place in accordance with the requirements of Article 32 (1) of Regulation (EU) 2016/679'.
(...)"

V

In order to establish the administrative fine to be imposed, the provisions of Articles 83.1 and 83.2 of the GDPR, which state:

'1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in

paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate, and dissuasive.

2.Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

(a) the nature, gravity, and duration of the infringement, considering the nature, scope or purpose of the processing operation concerned as well as the number of data subjects concerned, and the level of damage suffered by them.
(b) the intentional or negligent nature of the infringement.
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects.
(d) the degree of responsibility of the controller or processor, having regard to the technical or organizational measures they have implemented pursuant to Articles 25 and 32;
(e) any previous infringement committed by the controller or processor.
(f) the degree of cooperation with the supervisory authority to remedy the infringement and mitigate the possible adverse effects of the infringement.
(g) the categories of personal data concerned by the infringement.
(h) how the supervisory authority became aware of the infringement, whether and to what extent the controller or processor notified the infringement.
(I) where the measures referred to in Article 58(2) have been previously ordered against the controller or processor concerned in relation to the same matter, compliance with those measures.
(j) adherence to codes of conduct under Article 40 or to certification mechanisms approved pursuant to Article 42; and
(K) any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained or losses avoided, directly or indirectly, through the infringement.

In relation to Article 83(k) (2) GDPR, the LOPDGDD, Article *76, 'Penalties and corrective measures*', provides that:

'2. In accordance with Article 83 (2) (k) of Regulation (EU) 2016/679, account may also be taken of:

(a) the continued nature of the infringement.
(b) linking the offender's activity to the processing of personal data.
(c) the profits made because of the infringement.
(d) the possibility that the conduct of the person concerned might have led to the commission of the infringement.
(e) the existence of a merger by acquisition after the infringement has been committed, which cannot be attributed to the acquiring entity.
(f) the allocation to the rights of minors.
(g) provide, where this is not required, a data protection officer.
(h) the referral by the controller or processor, on a voluntary basis, to alternative dispute resolution mechanisms in cases where there are disputes between them

and any interested party.'

In accordance with the provisions set out above, and after completing the proceedings, for the purpose of determining the amount of the fine to be imposed in the present case for the infringement referred to in Article 83 (4) of the GDPR for which TYPEFORM is responsible, in an initial assessment, the following factors are considered to be present:

The international and non-local extent of the reported security gaps, since it should not be forgotten that they have affected a large number of countries and a very high number of people. Thus, in the first reported gap, the number of customers of the undertaking affected was 232.766 and, for the second, the number of customers affected was 2.892.786 and although the nationality of the customers was not available, if information on the place of residence was available, with more than 170 countries, including almost all those in the European Union.

The activity of the allegedly infringing entity is linked to the processing of data of both customers and third parties; this link is known as the entity is in constant contact and handles a large amount of data, which imposes a greater duty of care on it.

The degree of responsibility of the controller, taking into account the technical or organizational measures implemented that led to two security failures in a short period of time, resulting in the inadequacy of the existing and post-bankruptcy measures.

There is no evidence that the entity acted intentionally, although its action indicates a serious lack of diligence.

How the supervisory authority became aware of the breach, as the entity became aware of the security incidents quickly notified to the AEPD.

The degree of cooperation with the supervisory authority in order to remedy the infringement and mitigate the possible adverse effects of the infringement; as indicated above, the AEPD was promptly notified and appropriate measures were taken to remedy the situation created by communicating it to the supervisory body.

There is no record of a previous infringement committed by the controller or processor.

Considering the factors set out above, the assessment of the fine for the infringement of Article 32 (1) GDPR is EUR 100,000 (one hundred thousand euros).

Therefore, in accordance with the above, the Director of the Spanish Data Protection Agency RESUELVE:

FIRST: On the basis of the complaint processed under the IMI system, and in accordance with the facts and points of law contained in this act, adopt a draft decision on the penalty proceedings against TYPEFORM S.L., which will lead, where appropriate, to the

adoption of the following agreements:

1.Sanction TYPEFORM S.L. for an infringement of Article32 (1) GDPR, as defined in Article 83 (4) (a) GDPR, a fine of EUR 100.000 (one hundred thousand euros).

SECOND: In accordance with the procedure laid down in Article 60 of the GDPR, this draft penalty decision is transmitted through the IMI system without delay to the supervisory authorities concerned, informing them that, if no objections are raised within two weeks of the consultation, the mandatory decision on the penalty procedure will be adopted, in which the infringements listed in the grounds of law will be declared, with the imposition of the penalty indicated.

In accordance with Article 123 of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), interested parties may, in accordance with Article 46 of Law 29/1998 of 13 July on the Common Administrative Procedure of Public Administrations, lodge an appeal for reconsideration with the Director of the Spanish Data Protection Agency within one month of the date of notification of this decision or a direct administrative appeal before the Administrative Chamber of the Spanish Data Protection Agency, in accordance with the additional provision of the Spanish Data Protection Law, in accordance with the date of notification of this decision or a direct administrative appeal before the Administrative Chamber of the Fourth Section of the Audiencia, in accordance with the additional provision of the Spanish Data Protection Law, in accordance with Article 25 (5), as from the day following the notification of this decision or a direct administrative appeal before the Administrative Chamber of the National High Court, in accordance with of the Spanish Law, in accordance with (1).

Finally, we would point out that, in accordance with Article 90.3 (a) of the LPACAP, the final administrative decision may be suspended as a precautionary measure if the person concerned indicates his intention to bring an administrative appeal.

Mar España Martí
Director of the Spanish Data Protection Agency