□ Procedure No.: PS/00425/2020

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and based on

to the following

BACKGROUND

FIRST: On February 17, 2020, the director of the Spanish Agency for

Data Protection (hereinafter AEPD) agrees to initiate investigation actions

in connection with a security breach of personal data notified by the

MADRID CITY COUNCIL on February 12, 2020 and registration number

of entry of the AEPD 006633/2020 (hereinafter referred to as E/01657/2020),

regarding unauthorized access to proof of authorization as persons

residents of the Madrid regulated vehicle parking service.

Together with said security breach notification, the following was provided:

Supplemental Security Breach Summary Document

□

happened.

Internal notification of the Madrid City Council of vulnerability of

□

security, signed by the General Director of Sustainability and Control

Environment of the city council on February 10, 2020, addressed to the Directorate

General of Transparency (General Subdirectorate of Data Protection) of the

agency and referring in detail to the incident in question.

Screenshot of the unavailability of the Electronic Headquarters of the

□

AEPD at 6:23 p.m. on February 11, 2020 for notification of the present security breach.

SECOND: On March 4, 2020, the director of the Spanish Agency for Data Protection (hereinafter AEPD) agrees to initiate investigation actions in connection with a security breach of personal data notified by the MADRID CITY COUNCIL on February 27, 2020 and registration number of entry of the AEPD 009711/2020 (hereinafter referred to as E/01997/2020), relating to communication by a citizen via email about a claim that he had filed with the City Council in 2015 and that appears published on the Internet by doing a search through Google.

The City Council states that there had been changes in the System of Information on Suggestions and Complaints (SyR) for sending responses tions to the SyR presented at the Town Hall. Among these modifications was that In the link that citizens receive to access their answer, it would be required an ID with two validation fields. This new system was launched Cha in August 2019.

The City Council, aware that some users had published on social networks them the link provided and as a result of the citizen's communication they proceeded from the Autonomous Information Technology Body Madrid City Council (IAM) to the elimination of

all indexing of pages in any internet search engine, acting as a priority-mind over Google. This solution works correctly for all S&R responses. given since August 2019.

Regarding the searches carried out through other search engines different from

Google, IAM has taken action so that no reply links that the

user has decided to publish on any internet page, such as forums, blogs, etc.

This action through the robot.txt file affects all search engines.

THIRD: In view of the notified facts and the documents provided by the

City Council, the General Subdirectorate of Data Inspection proceeded to the

carrying out preliminary investigation actions to clarify the

facts described in the previous sections, by virtue of the investigative powers

granted to the control authorities in article 57.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter RGPD), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the Law

Organic 3/2018, of December 5, on the Protection of Personal Data and guarantee of

digital rights (hereinafter LOPDGDD), having knowledge of the

following ends:

INVESTIGATED ENTITIES

MADRID CITY COUNCIL (hereinafter the investigated), General Directorate of

Transparency, with NIF P2807900B and address at C/ Alcalá 45, 28014 Madrid.

RESULT OF THE INVESTIGATION ACTIONS. E/01657/2020

Date of notification of the security breach in the AEPD: 02/12/2020

BACKGROUND

The investigative actions have been carried out by sending

request for information from the AEPD and response to it by the

investigated according to the following time sequence:

Information request to the investigated, dated February 24, 2020 and

1.

AEPD exit registration number 017919/2020.

Respondent's response, dated July 22, 2020 and number of

two.

AEPD entry registration 025844/2020.

(It is noted that the associated Investigation File (E/01657/2020) has been

been affected, in terms of administrative deadlines, by the provisions of Royal

Decree 463/2020, of March 14, declaring the state of alarm)

Analyzing the terms that make up the aforementioned response of the respondent,

deduces:

Yo. Regarding the facts:

□

□

□

□

The investigated informs that its Subdirectorate General for Architecture and

Computer Security communicated on February 7, 2020 by mail

email to the General Directorate of Sustainability and Environmental Control,

responsible for the regulated vehicle parking service in Madrid

(hereinafter SER), the information received on February 6, 2020 from the

National Institute of Cybersecurity (hereinafter INCIBE) referred to a possible

security incident affecting the website:

https://movilidad.madmovilidad.es

The incident, which in turn had been reported by a user to INCIBE, consisted of the possibility of accessing proof of authorizations of third-party residents of the SER, in which the name, surnames and DNI of the the authorized person, as well as the vehicle registration, through the URL: https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imimpresionJustificantePeriodo.pdf?idPeriodo=2046824&tipoAuthorizacion=1

The investigated exposes that the vulnerability detected was confirmed the same February 7, 2020 and was referred to the printing of supporting documents that were issued so that users have evidence of their authorization to resident in the BE. The incident was that the numbering of the URL was consecutive, so the sequential change of a digit allowed access to personal data of third parties.

The investigated identifies the involvement of four treatment managers in the treatment activity that suffered the security breach that occurred correspond to the concessionaire companies that provide the service of SER management under the indirect concession system:

Company 1: ***COMPANY.1

Company 2: ***COMPANY.2

Company 3: ***COMPANY.3

Company 4: ***COMPANY.4

The aforementioned treatment managers of the investigated maintain that:

On February 7, 2020, the investigated reported the incident to them, as either

responsible for the treatment, and that, after verifying its existence, automatically and as a preventive measure they disabled the page of procedures of the SER, preventing access to the page, as well as to any information contained therein until determining the origin and scope of the

Unauthorized access.

On February 8 and 9, 2020, they carried out an audit of the

either

application of SER procedures to determine and verify the existence of

other possible unreported fraudulent access.

On February 12, 2020, they proceeded to deploy in environments not

either

productive of the solution adopted for the resolution of the incidence and

They transferred her to the investigated person so that she could validate her as responsible for the

treatment.

On February 13, 2020, after checking the validity of the solution

either

adopted, they deployed it in the production environment, it was validated by

of the investigated and was enabled on the web page of SER procedures.

□

□

□

The investigated affirms that all the available logs of accesses to

supporting documents from the internet, without having detected systematic access to the

exposed information. The investigated asserts that unauthorized access of which there is evidence are those carried out by the person who communicated the INCIBE vulnerability, iterating over the “idPeriodo” parameter in the URL indicated:

https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imimpresionJustificantePeriodo.pdf?idPeriodo=2046824&tipoAuthorizacion=1

https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imimpresionJustificantePeriodo.pdf?idPeriodo=2046823&tipoAuthorizacion=1

https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imimpresionJustificantePeriodo.pdf?idPeriodo=2046822&tipoAuthorizacion=1

https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imimpresionJustificantePeriodo.pdf?idPeriodo=2046821&tipoAuthorizacion=1

The respondent reports that this method, which allowed access to information did not enable any modification or deletion of the data involved in the security breach.

Those in charge of the treatment of the aforementioned investigation state that:

The web application for SER procedures is based on a either MVC architecture (model-view-controller) in which Spring is used WebFlow with JSP (Java Server Pages), in which all the Requests were made using the HTTP POST method (procedure whereby the browser sends information to the server in a non-visible way in the URL), except downloading the PDF of the authorization receipt of the SER involved in the security breach, which was carried out using the HTTP GET method (procedure by which the browser

sends information to the server visible in the URL).

Access to said functionality was produced by pressing a button on the

either

SER authorization form called "Print receipt",

after which a request with HTTP GET method was launched to the server

with the following parameters:

a)

“idPeriodo”: identifier with unique number of a period

associated with an authorization. This identifier is generated internally and

it is never shown in the forms to the user. This identifier must

belong to an active period, otherwise the receipt cannot be

Discharged.

b)

“tipoAutorizacion”: depending on the type of authorization this takes

one value or another, being the value “1” type of resident authorization.

When the request arrived at the server, it generated the corresponding PDF

either

associated with the "idPeriodo", that is, contained as a parameter in the

request, and once the file was generated, the server returned what was appropriate to the

browser for the download to take place on the client computer.

In the case of a request made through the HTTP GET method, the

request was visible in the address bar of the web browser with the following format:

https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imimpresionJustific

antePeriodo.pdf?idPeriodo=nnnnn&tipoAuthorizacion=n

Therefore, in case of altering the indicated parameters in the

either

mentioned download link, accessing it through a

browser, it was possible to download the PDF of proof of

SER authorization for a certain period. In any case, the new

identifier entered must exist, that is, belong to a period in

active status and be for an authorization of the same type as indicated

in the second parameter “tipoAuthorizacion”.

Even if the existing identifier is manually varied, this does not

either

implies that the new identifier exists because:

the periods, among other functionalities, can be

□

down by the users themselves.

the status of the period (which can be: in process, pending

□

payment, notification pending, active, expired, pin pending,

canceled, rejected, sent home or modified), in order to download the PDF of proof of authorization from the SER,

must be the active one at the time the transaction was made.

download request in question.

The respondent states that the number of affected data records is

four, that is, exactly the number of people affected by the

incident, of which it confirms that there was access by the third party that

notified INCIBE:

or Name and surnames.

or ID.

o Vehicle registration.

o Name of the SER area to which the authorization corresponds.

The respondent maintains that she is not aware of the use by third parties of

personal data obtained through unauthorized access to data

personal happened.

The investigated party alleges that the security breach notification to the AEPD was

produced late, on February 12, 2020, due to an error in the

server of the electronic headquarters of the AEPD on February 11, 2020. The

investigated provides a screenshot of said error on the date indicated to the

6:23 p.m.

□

□

□

ii. Regarding the measures prior to the occurrence of the security breach:

□ Regarding the accommodation of the application of procedures of the SER, those in charge

of the treatment of the investigated state that she is housed in a

external provider of information and communication technology services communication (US corporation: (...), with its services: Managed

Services), whose digital infrastructure consists of a private cloud environment

safe, and that has a backup center in active - passive mode.

Also, as reported, said provider has implemented and certified

the following standards:

o For data center services:

□

ISO 27001 - Information security management.

□

ISO 22301 - Business continuity.

PCI DSS (Industry Data Security Standard)

payment card).

□

SOC 1 / SOC2 Reporting (Reporting Control

financial / security compliance, confidentiality,

integrity, availability and privacy).

o For managed services:

□

□

□

ISO 27001 - Information security management.

ISO 22301 - Business continuity.

ISO 20000–1 - Requirements for management systems of services.

According to those in charge of the treatment of the investigated, this provider of external information and communication technology services contemplates a global process of management of incidents on action, escalation and communication to clients for the necessary case, including the notice to the corresponding authorities depending on the type of incident. Also, According to its version, this provider includes a contingency plan, training and annual continuity testing plan, contemplating, according to certain results, an analysis and an action plan for improvement.

- Regarding the architecture of the application of procedures of the SER, those in charge of the treatment of the investigated state that in the access to the procedures:

o Registration of vehicle authorization for residents:

https://movilidad.madmovilidad.es/TramitesPortalWeb//app/altaResidente-flow?execution=e1s1

o Consultation and management of authorizations:

https://movilidad.madmovilidad.es/TramitesPortalWeb//app/consulta-flow?execution=e2s1

a cookie is generated on the client, called "jsessionid", which saves a unique session identifier that is retrieved on each request to the server.

In such a way that to be able to visualize the compromised information in this case, it is required that the forms complete:

o Registration of vehicle authorization for residents:

 Type of identification document of the holder.

 Number of the holder's identification document.

 Vehicle registration.

 CAPTCHA test (Verification image à Code of

check).

According to those in charge of treatment of the investigated, in order to continue,

the person must appear as registered in the census database

of inhabitants of the investigated and appear as the owner of the vehicle with that

registration in the database of the General Directorate of Traffic of the Ministry

inland. In that case, according to said version, the user will be able to choose the period

duration and register the corresponding authorization in the SER.

o Consultation and management of authorizations

 Type of identification document of the holder.

 Number of the holder's identification document.

 Authorization code [only known by the user when

perform the registration / payment of the authorization of the SER according to

defend].

 Registration or ford.

 Email.

 Email confirmation.

 CAPTCHA test (Verification image à Code of

check).

Finally, according to those in charge of treatment of the investigated, in addition to

If correct data is required, it is insisted that all requests made to navigate and communicate between the different pages and the server is performed via HTTP POST method, except for the functionality related to the printing of the proof of authorization of the SER for a period that has generated the present security breach (performed by the HTTPGET method).

□

The respondent provides a copy of the inventory of treatment activities (IAT) partial, in which the personal data compromised in the security breach and with the following information:

o Treatment activity: Regulated parking areas.

o Responsible for the treatment: General Directorate of Sustainability and Environmental Control of the Madrid City Council, with its postal address full contact.

o Purpose: Parking management on public roads.

o Data Protection Delegate: General Directorate of Transparency of the Madrid City Council.

o Category of interested persons: Citizens and residents, legal representatives, taxpayers and obligated subjects, persons of contact and vehicle owners.

o Personal data: Identification (name and surnames, DNI/NIF, address, telephone and private email), social

(property and possessions), commercial information (activities and

business), economic-financial (bank data and credit cards

credit) and other types of data (vehicles-registration).

o Assignment recipient bodies: General Directorate of Management and

Traffic Surveillance (Mobility Ordinance for the city of

Madrid) and Administration of Justice and its support bodies.

o International data transfers: No.

o Technical and organizational security measures: Security Policy

of the Information of the Madrid City Council and its Organisms

Public, approved by agreement of the ANM Governing Board

2017/36, of May 24.

o Legitimation for data processing: Public interest

(allocation of vehicle parking space on the road

public. Promote sustainable mobility) and consent of the affected party.

o Data conservation periods: The identifiers are not deleted,

are kept for consultation in the history.

□

□

There is no information about their data processors.

The respondent states that, within the framework of her project "Verification of the degree of adequacy of the Madrid City Council to the General Regulations of Data Protection (RGPD) and Organic Law 3/2018, on Data Protection Personal and guarantee of digital rights (LOPDGDD) and implementation of a methodology for carrying out risk analysis and evaluation of impact of data protection”, a preliminary analysis of the risks of the treatment activity “Regulated Parking Areas”, the result of which has obtained its rating as low risk.

In any case, the investigated party does not provide said risk analysis (RA) referring to the aforementioned treatment activity “Regulated Parking Areas” of its IAT and involved in the incident in question.

The investigated does not provide, nor does it motivate said absence, regarding possible need and execution of impact assessment related to the protection of data (EIPD) referring to the aforementioned treatment activity “Areas of Regulated Parking” of your IAT and involved in the incident in question.

iii. Regarding the measures after the event of the security breach:

iii.a. Of a corrective nature (reactive to correct the security breach):

□

□

Those in charge of the treatment of the investigated express that the first measure adopted on February 7, 2020 by the technicians of the application of procedures of the SER, after receiving the notification of the analyzed vulnerability, it was disable the application preventing any access to both the page and the information guarded. According to his account, all accesses to the application from that moment they were resolved with the error codes “HTTP Status 404 -Not Found” and “HTTP Status 503 - Service unavailable” until the implemented the final solution on February 13, 2020.

Those in charge of the treatment of the investigated defend having carried out carry out an analysis of the risk and the impact on possible unauthorized access to the web application for SER procedures and specifically to the functionality of the download of proof of authorization from the SER per period.

Those in charge of the treatment of the investigated relate the aforementioned analysis as follows:

o Threat identification:

- SER procedures application: function to download the PDF of the proof of authorization from the SER in a period carried out by HTTPGET method.

- Accesses to the application: collection and analysis of all Requests made between January 5, 2020 and December 7, February 2020 (date of incident).

o Risk assessment:

- Application of SER procedures: the application of modification or deletion of personal data in the event of unauthorized access to a download of the authorization PDF of the BEING of a third party. It is required to know the functionality and the format of the URL to invoke and that exists correspond between the “idPeriodo” and “tipoAuthorizacion” parameters, which is not direct in all cases (not strict correlation).

 Access to the application: it is established as a cataloging criterion of risks give scores from 0 (very low) to 5 (highly suspects), on which a purge will be applied and access evaluation.

o Treatment of risks:

 Application of SER procedures: disable the web application until the incident was resolved, avoiding potential new unauthorized access.

Realization of technical developments in the application in the field of sending the information (change of the HTTP GET method) and Encryption of information using an algorithm.

After verification of the solution, the non-existence of these risks and the application was rehabilitated.

 Access to the application:

- Access considered authorized: 13,846 risk accesses 0, 37 risk accesses 1 and 36 risk access 2.

- Accesses considered unauthorized: 14 accesses of risk 3, 0 accesses of risk 4 and do not consist of risk 5. Of 12 of the risk 3 accesses, 4 are obtained proof of authorization from the SER that coincide with the identifiers notified by INCIBE and object of this security breach. The other 2 risk accesses

3 correspond to the same IP address (protocol internet), ***IP.1, possibly masked by a VPN (Virtual Private Network) due to your geolocation, and probably belongs to whoever identified the incidence.

It is established that the committed data correspond to 4 natural persons, one of them possibly being the one identified the incident itself. Considering the number of accesses and the dates and times, are considered accesses in a manually, without the use of massive, iterative or automated.

□

Those in charge of the treatment of the investigated inform that the method HTTP GET for the printing of authorization receipts from the SER was changed by the HTTP POST method, this being the main technical measure with which the risk was assessed as mitigated.

Said data processors establish that this variation was implemented, tested and verified in the pre-production environment on 12th February 2020, without legible or identifying parameters that can be manipulated in the URL at the request level.

Finally, those in charge of the treatment of the investigated state that, not having detected vulnerabilities, they implemented the solution to the environment of production and subsequently enabled it in the web application on 13th February 2020, in such a way that, from that moment, the service was recovered not being able to invoke the printing of proof of authorization from the SER by the

HTTPGET method.

In the security breach notification to this AEPD and in its documentation

attached, the investigated expressly stated that the security breach was not

entails a high risk for the rights and freedoms of natural persons

affected and that it is a small number of them, so it has not

considered necessary the communication and has not made it.

iii.b. Of a preventive nature (proactive to avoid a recurrence of the gap in

security):

□

Those in charge of the treatment of the investigated state that, in addition to the

implementation of the HTTP POST method for printing receipts

authorization of the SER, the "idPeriodo" parameter is now accompanied by two

new parameters: the authorization code and the payment burst. With that,

expose the existence of a unique identification of each receipt generated.

These data processors maintain that the correlation between the three

set parameters is only known by the application. They add that the three

parameters are combined into one, which is encrypted using AES encryption

(advanced encryption standard) and a key stored on the server and

unknown at all times by clients, depending on their version. When the

request to print proof of authorization from the SER to the server, the chain is decrypted with the same key in order to obtain it and offer it to the application user.

FOURTH: On November 30, 2020, the Director of the Spanish Agency of Data Protection agreed to initiate a sanctioning procedure against the CITY COUNCIL DE MADRID, for the alleged infringement of articles 32,33,34 and 35 of the RGPD in in relation to article 5.1.f) of the RGPD and for the alleged infringement of article 5.1.f) of the GDPR.

FIFTH: On 12/29/2020, the respondent presented allegations to the settlement agreement initiation stating, among others, that the initiation agreement is null and void of full rights by initiating in a single file two different acts carried out by different responsible parties, for which he requests the filing of the file due to lack of responsibility of the Madrid City Council in the imputed infractions.

PROVEN FACTS

FIRST: It appears as responsible for the treatment in the Registry of Activities of Treatment (RAT) of the treatment operation related to “Suggestions and Claims” (SyR) the General Directorate of Transparency and Quality, attached to the Government Area of the Deputy Mayor's Office, as stated in the organizational structure of the City of Madrid.

SECOND: It appears as responsible for the treatment in the Registry of Activities of Treatment (RAT) of the treatment operation related to “Areas of Regulated Parking” (ZER) the General Directorate of Sustainability and Control Environment, attached to the Government Area of Environment and Mobility, as recorded in the organizational structure of the Madrid City Council.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of control, and as established in arts. 47 and 48.1 of the LOPDGDD, the Director of

The Spanish Agency for Data Protection is competent to resolve this

process.

II

The art. 89.1.d) of Law 39/2015, of October 1, on Administrative Procedure

Common to Public Administrations (LPACAP) states the following:

<Article 89. Resolution proposal in sanctioning procedures.

1. The investigating body will resolve the completion of the procedure, with a file of the

actions, without it being necessary to formulate the resolution proposal,

when in the procedure instruction it becomes clear that there is any

of the following circumstances:

d) When it does not exist or it has not been possible to identify the person or persons

responsible or appear exempt from responsibility.>

The art. 28.1 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector

(hereinafter LRJSP) states the following:

< Article 28. Responsibility.

1. They may only be sanctioned for acts constituting an administrative infraction.

natural and legal persons, as well as, when a Law recognizes their capacity to

to act, the affected groups, the unions and entities without legal personality and the

independent or autonomous estates, which are responsible for them

title of fraud or guilt>.

Article 70 of Organic Law 3/2018, of December 5, on Data Protection

Personal and guarantee of digital rights, states the following:

<Article 70. Responsible subjects.

1. They are subject to the sanctioning regime established in Regulation (EU) 2016/679

and in this organic law:

a) Those responsible for the treatments.

b) Those in charge of the treatments.

c) The representatives of those responsible or in charge of the treatments do not

established in the territory of the European Union.

d) Certification entities.

e) The accredited entities for the supervision of codes of conduct.

2. The sanctioning regime will not apply to the data protection delegate

established in this Title>.

Taking into account the aforementioned articles and the proven facts, in the present case,

in relation to the allegation (among others) indicated above that the agreement of

beginning suffers from the vice of nullity of full right when initiating in a single file two

different acts carried out by different responsible parties, it must be accepted and

file the sanctioning procedure, since the legal entity

imputed does not correspond to the person responsible for the analyzed treatments.

However, it is meant that notification of the two security breaches

(SyR and ZER treatments) in accordance with the provisions of article 33 of the RGPD, were notified to this AEPD by the Madrid City Council as

"Responsible" for them.

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of the sanctions whose existence has been proven, the Director of the

Spanish Data Protection Agency RESOLVES:

FIRST: FILE this sanctioning procedure.

SECOND: NOTIFY this resolution to the MADRID CITY COUNCIL, with

NIF: P2807900B.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the

LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the

Director of the Spanish Agency for Data Protection within a month from

counting from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided in article 46.1 of the

aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP,

may provisionally suspend the firm resolution in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registers provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the documentation proving the effective filing of the contentious appeal-administrative. If the Agency was not aware of the filing of the appeal contentious-administrative within a period of two months from the day following the notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency