

☐ Procedure No.: PS/00091/2020

## RESOLUTION OF PUNISHMENT PROCEDURE

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

### BACKGROUND

FIRST: CITY COUNCIL OF \*\*\*LOCALITY.1 (hereinafter, the claimant) with  
date 05/07/2019 filed a claim with the Spanish Agency for the Protection of  
Data. The claim is directed against GIRONA INTEGRAL EXPRESS, S.L. with NIF  
B17770991 (hereinafter GIEXPRESS), for  
the following facts according to  
statements of the claimant: That on 03/19/2019 the Environment technician of the  
City Hall of \*\*\*LOCALIDAD.1 located a waste dump outside the  
containers with garbage remains, delivery notes and documentation of delivery of  
parcel of the company TIPSA GIRONA (a total of 212 pages) in which they appear  
names, surnames, DNI and address of natural persons.

The city council required an audience with the person in charge of said company to collect the  
documentation and give it the appropriate treatment. That he has not appeared within the term  
required.

And, among other things, attach the following documentation:

Photographs of the containers with garbage outside of them.

☐

☐ Copy of the request from the City Council of \*\*\*LOCALIDAD.1 to the respondent  
dated 03/27/2019.

☐ Acknowledgment of receipt of the request with acceptance date 03/29/2019 by Mr.

A.A.A. with NIF \*\*\*NIF.1.

□ Copy of the delivery notes and delivery documentation from TIPSA GIRONA where contain data of name, surnames, NIF, postal address and telephone number of contact of natural persons.

SECOND: Upon receipt of the claim, the Subdirector General for

Data Inspection proceeded to carry out the following actions:

On 04/22/2019, the complaint was transferred to TRANSPORTE INTEGRAL DE PAQUETERIA, S.A., in the proceedings with reference E/05813/2019.

On 07/12/2019, TRANSPORTE INTEGRAL DE PAQUETERIA, S.A. refer to this Agency the following information and statements:

1. That in order to provide its services, its business model is focused on the creation of a national distribution network of agencies of merchandise transports.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

2/20

2. That TRANSPORTE INTEGRAL DE PAQUETERIA, S.A. proceeds to the signing of a contract with all existing agencies.

A collaboration contract is provided between TRANSPORTE INTEGRAL DE PACKAGE, S.A. and GIEXPRESS dated 10/21/2004. In your clause seventh is manifested:

“SEVENTH.- This contract does not constitute a corporate or agency relationship, company or joint or joint activity between TIPSA and GIE, maintaining each of the parts its full independent and differentiated personality legal, capacity to act, activity, development and operation,

responding, above all, as far as GIE is concerned, of all the consequences derived from its industry or business, whose risk and venture fully assumes with total indemnity from TIPSA, which must be protected from third parties of any harmful consequence derived from their own actions or their personal or attributable to him for any reason, including agreements or pacts that it concludes with those, responding with unlimited character for all this, including in the scope of its responsibility the damages and own damages and damages to third parties in personnel, facilities and properties. As an obvious consequence of the foregoing, this contract does not imply a bond or employment relationship of any kind, principal, joint or subsidiary between TIPSA and GIE and its staff, who will assume and be responsible for everything entails or is inherent to their own employment status and that of their workers or dependents, regardless of the nature of the relationship that unites him with they...

In order for the TIPSA agreed waiver of liability to take place, GIE, undertakes to state before its staff, third parties and organizations who is solely responsible for the activity carried out in performance of this contract, and that TIPSA bears no responsibility.”

Novation of the collaboration contract signed on 10/21/2004 is provided between TIPSA and GIEXPRESS dated 05/01/2008. In its fifth clause in relation to the protection of personal data and commitments of confidentiality, it is stated:

“In relation to the data provided by TIPS@ to GIEXPRES, the former has the condition of responsible for the file that will be constituted with the data processed and GIEXPRES will hold the status of data processor...

In relation to the data provided by GIEXPRES, to TIPS@, the former has the

condition of responsible for the file that will be constituted with the data processed

and TIPS@ will hold the status of data processor...

Likewise, both parties undertake to deal with the maximum

confidentiality how much personal data is provided with

reason for this service contract, committing to treat them as

in accordance with the measures established in the current regulations for the protection of

data as well as to adopt in the future as many security measures as are

required by laws and regulations intended to preserve secrecy,

confidentiality and integrity in automated data processing

personal.

....

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

3/20

Both parties undertake to inform their staff, collaborators and

subcontractors of the obligations established in this contract on

confidentiality, as well as the obligations related to data processing

of a personal nature GIEXPRES and TIPS@, will carry out as many warnings and

will sign as many documents as necessary with their staff and

collaborators, in order to ensure compliance with such obligations.

Once the established contractual provision has been fulfilled, both parties

oblige with respect to the other to destroy or return all data, media or

documents held by the counterparty, including all data of a nature

personnel object of the treatment that at that time were in their possession,

except those that by legal imperative have to be preserved.”

1. States, among others, that the following decisions have been made:

a. Review of the service lease contract signed with

GIEXPRESS.

b. Review of whether the contents of training in the field of Protection of

Data is adjusted to the entity's operations.

2. Provide the answer sent by GIEXPRESS to TIPSA as an attachment to the email

email sent by \*\*\*EMAIL.1 dated 06/25/2019 and the following

manifestations:

a. That the company they have contracted for the periodic collection of

waste of organic matter, plastic and paper is RECOVERIES

MARCEL I NAVARRO FILLS, S.L. with NIF B17255639.

b. That your company has never deposited delivery notes or documentation of

customers anywhere other than at your facility for your

destruction.

c. That the only explanation they find for this incident is that a

supplier of your company has deposited the documents in the

container of \*\*\*LOCATION.1.

d. States that in relation to the receipt of the electronic notification

by the City Council of \*\*\*LOCALIDAD.1, there was a bad

channeling of the mail received in \*\*\*EMAIL.2, being the mail that

have to receive telematic notifications from some

agency such as Treasury, Social Security or others the following;

\*\*\*EMAIL.1, which is your personal email and, understanding, that it was a

sanction by some radar he forwarded it to his advisor from the account

\*\*\*EMAIL.2 and his advisor responded to that same account, losing

so the track.

and. Who understand that everything has been a human error on the part of their supplier who was unaware of the causes on the law of protection of personal information.

F. That for their part they will proceed to review the processes of this type of documents so that no one is lost at any time delivery note. That in fact, this is already impossible to happen since their providers no longer carry physical sheets but go with telephones mobiles.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

4/20

3. That they requested GIEXPRESS the contract with the supplier that is in charge of the documentary destruction but it has not been sent to them for what they suppose that this contract does not exist.

4. That they have proceeded to adopt the following measures:

a. That an organizational restructuring has been carried out within the your entity to integrate surveillance and compliance in terms of data protection within the legal or compliance department regulations from the quality department where he was.

b. That, in the face of contractual breaches detected by GIEXPRESS. a proceeding will be opened clearance of responsibilities to it.

c. They state:

“TIPSA has given instructions to its department of Computing to enable a specific online platform in compliance with Data Protection, as already exists in terms of compliance in labor matters, in which they will have access all those third parties that work for TIPSA, which must attach in it all those documents that prove that they comply with all those points that the same platform will anger them requesting automatically, in order to be able to justify a truest way, that each company has the guarantees legal requirements requested by TIPSA to be able to work, such as by example, having a Record of Activities, complying with the duty of information, have a Risk analysis carried out, Impact Assessments, International Data Transfers, etc. etc..

Thus, if at the moment that the same platform detects that it is not find all the requested Documentation, or it is incorrect, for part of it, a signal or distinctive sign will be elaborated by which will be notified in order to request said documentation and if the lack or error in the documentation persists over time, proceed even by of TIPSA to the resolution of the corresponding contracts that remained in force or the impossibility of contracting with it.”

5. Provides a signed contract for the processing of character data personnel dated 05/25/2018 between INTEGRAL TRANSPORT OF PACKAGE, S.A. and GIEXPRESS where it is collected:

a.

b.

“In relation to the data provided by TIPSA to GIRONA INTEGRAL

EXPRESS, S.L., the former has the status of Responsible for

File that is constituted with the processed data and GIRONA INTEGRAL

EXPRESS, S.L will hold the status of Treatment Manager...”

“In relation to the data provided by GIRONA INTEGRAL EXPRESS,

SL to TIPSA, the former has the status of Responsible for the File

that is constituted with the processed data and TIPSA will hold the

Condition of Treatment Manager...”

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

5/20

c.

d.

and.

F.

“In particular, the person in charge of the treatment will apply the measures of

technical and organizational security detailed in Appendix I of the

this Agreement.”

“...the Manager guarantees the Manager that his staff as well as

The persons authorized to process the Personal Data are

undertake, expressly and in writing, to respect the

confidentiality and compliance

security measures

corresponding, of which it is necessary to inform them conveniently,



keeping the documentation available to the Responsible

proof of compliance with this obligation. Likewise,

guarantees the necessary training in the field of personal data protection.

its personnel and of the persons authorized to treat the Data of

personal character."

"Once the provision of the Services has been completed, the Person in Charge of the

treatment will destroy or return to the person in charge of the treatment or to the

manager who designates in writing the Responsible for the aforementioned Data

of a personal nature (as indicated by the Responsible), as well as

any support or documents containing the Data of

personal character object of treatment within the framework of this

Contract.

If the person in charge opts for the destruction by the person in charge of the

treatment of personal data as well as any

support or documents containing the Character Data

personnel, the person in charge of the treatment must certify its destruction

written..."

"The person in charge of the treatment recognizes the person in charge of the treatment

the power to subcontract with third parties, in whole or in part, the

Services object of this Contract."

g. Provides Appendix I of the contract with the following security measures

technical and organizational among others:

Yo.

ii.

iii.

"The person responsible for the file or treatment will adopt the measures

necessary for the staff to know in a way understandable safety regulations affecting the development of its functions as well as the consequences in which it could incur in case of non-compliance.”

“Whenever any document or support is to be discarded that contains personal data must proceed to its destruction or erasure, through the adoption of measures aimed at preventing access to the information contained in the itself or its subsequent recovery.”

“While the documentation with personal data does not is stored on storage devices established in the previous article, for being in the process of review or processing, either prior to or after filing, the person in charge of it must guard it and prevent it from being accessed at all times by unauthorized person.”

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

C/ Jorge Juan, 6

28001 – Madrid

6/20

6. Document “Operating manual instruction / Delivery of shipments operational” dated 01/01/2019 whose scope, as stated in the document, is all the TIPSA agencies and where in its section “3.10 Digitization and Filing of Delivery Notes” includes:

a.

In order to comply with current legal regulations on claim deadlines for transport services, the destination agency undertakes to digitally file in its facilities all delivery notes of the shipments entrusted to you by the Tipsa Network for its distribution, at least for 24 months. The destination agency will be responsible for maintaining due diligence in the custody and conservation of said delivery notes, for compliance with third parties and judicial and/or administrative bodies of the legal obligations of exhibition of these documents before them.”

7. Survey completed by GIEXPRESS on May 25, 2018 is provided in whose header appears the title "AUDIT MEASURES IMPLEMENTED IN YOUR COMPANY ABOUT CHARACTER DATA PROTECTION PERSONAL” and where this entity states that:

a.

Workers have been informed in accordance with the new regulations on Data Protection.

b. Rules have been defined for the destruction of data carriers and documents.

On 01/27/2020, GIEXPRESS sends this Agency the following information and manifestations:

1. That they became aware of the incident on June 18, 2019 through from a TIPSA statement.
2. That the carrier that caused the incident was hired as a reinforcement given the increase in the volume of work in that period.
3. It states that “...conversations were held with the carrier involved, to determine the motivation for the irregular deposit of the

documentation outside the container, on public roads. This entity, after investigation of the event, concluded that said carrier, for unaware, proceeded to improperly dispose of it in the understanding that they would be disposed of by the municipal collection service.

This entity concluded that it was a human error due to lack of diligence, without the appearance of bad faith or intent to harm data privacy contained in said documents and without giving rise to any benefit economic cost of such action for the responsible carrier.”

1. That the identification of the carrier that discarded the documents is D.

BBB with NIF \*\*\*NIF.2.

2. In relation to the carrier that discarded the documents, it states that “This employee has not undergone data protection training.”

3. That said carrier had the information in physical documentation because in

At the time of the incident, the management of delivery notes and deliveries was in a

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

7/20

moment of technological adaptation and was still in the process of change from physical documentation to the use of a mobile application.

4. That said process of technological innovation in the way of managing

delivery notes was launched on May 6, 2019 until July 9, 2019

moment from which the physical documentation was completely dispensed with.

5. That prior to the actual knowledge of the incident they already had a

provider of periodic collection services at its facilities with

RECUPERACIONES MARCEL I NAVARRO FILLS, S.L using containers

sealed for the introduction of documentation with personal data or

confidential. That said contract is still in force today.

A signed contract dated January 2, 2019 is provided, according to its translation

unofficial of the Catalan, of waste treatment with the company

RECOVERIES MARCEL I NAVARRO FILLS, S.L

OBSERVATIONS: Said contract does not seem to include the destruction of documents.

1. That your entity had a data protection consultant.

A contract signed on May 21, 2018 for the commissioning of

treatment with CENSOR CONSULTING, S.L. being the files included in

the order of Human Resources, Payroll and personnel and curriculum vitae

and the service provided is that of "LOPD Consultant".

2. That they had already transferred to the employees a Commitment to

Confidentiality and an Internal Communication.

Documents dated May 21, 2018 and signed by 13

employees regarding Information to Users and the duty of professional secrecy

where it is stated that:

"The supports that contain the data of the File must be stored

in places to which unauthorized persons do not have access for the use of the

File."

OBSERVATION: This document is not signed by the carrier

identified that discarded the documents.

3. That on July 8, 2019, the following document was sent to

the entire template.

An Internal Circular signed by employees, undated and in relation to the

data protection, in which it establishes in point 2:

“Disclosure of processed personal data should be avoided, remaining

The unauthorized transfer of any of them is expressly prohibited.

...

Any document that can be made within the facilities of

GIEXPRES with personal data must be deposited in the

sealed container for proper subsequent destruction.

OBSERVATION: This document is not signed by the carrier

identified that discarded the documents.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

8/20

4. That in April 2019 a consultant specializing in the

regulatory compliance contracting the service of adaptation to the regulations

in force regarding data protection.

A copy of the contract signed and dated April 25, 2019 is provided with the

company PROFESSIONAL GROUP CONVERSIA, S.L.U.

5. That they proceeded to document the incident on June 19, 2019

concluding that it was not proceeded to communicate it to this Agency or to the

interested.

Provide a copy of the document entitled "Communication Model of the

Resolution before the Violation or Security Breach" dated June 19,

2019 and addressed to GIEXPRESS where in the section "Conclusion of the analysis of

the operation" it is stated that:

“-In accordance with article 4 section 12 of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, regarding the protection of natural persons with regard to data processing personal information and the free circulation of these data and by which the Directive 95/46/CE (hereinafter RGPD) is a security violation due to an accidental loss of personal data.

-It may involve unauthorized access to personal data.

-Taking into account the volume of files and people affected, the type of data and the impact (exposure) is not reported to the Control Authority nor the communication to those affected by the incident of security.”

The “Actions Carried Out” section includes:

“-The security breach has been documented in accordance with the article 33.5 RGPD

-Assessment and Analysis of the incidence to verify the probability that the violation constitutes a risk to the rights and freedoms of individuals physical

-No notification to the control authority as established in article 33 of the RGPD and the analysis carried out”

6. That the remote training service in Privacy and Information Management was contracted. Information as of July 23, 2019 for two workers.

A copy of the signed contract dated July 23, 2019 is provided in which section of "Object of the contract" is collected "TELEFORMATION VIA ELECTRONICS THROUGH A TRAINING PLATFORM” and the section on “contracted courses” includes the course with the title “Privacy and management of the information” with a duration of 56 h.

7. That on January 20, 2020, all employees have been notified of a Communiqué in order to reinforce the importance of diligence in the processing of personal data.

8. A Record of Activities is provided, composed exclusively of the following sections:

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

9/20

a. In relation to the data of the data controller and his delegate data protection:

Yo. Commercial and contact data of the person in charge of the Treatment.

ii. Data of the Data Protection Delegate.

b. In relation to the data of the person in charge of the treatment and his delegate of Data Protection:

Yo. Commercial and contact data of the Treatment Manager.

ii. Data of the Data Protection Delegate.

c. In relation to international data transfers:

Identification of the country and international organization.

Yo.

d. In relation to security measures.

Yo. Security measures implemented for this treatment.

9. Risk analysis and management is provided dated June 13, 2019 where pick up:



a. In the section "Identification of data processing personal" among others include "Management of shipments and deliveries".

b. In the section "Initially Planned Measures" in relation to the "Management of shipments and deliveries" lists the measures planned initially that, among others, consist of:

Yo. In relation to the potential risk scenario with code RO.01 and description "The general regulation on the right to the protection of personal data" it is collected that "There is NO document available that reflects the measures of security that the company must adopt to minimize the risks,..."

ii. In relation to the potential risk scenario with code ROS.05 and description "There is unauthorized access to personal data" is states that "NO security measures have been implemented, nor physical or computerized, to the information systems for prevent unauthorized access"

iii. In relation to the potential risk scenario with code ROS.08 and description "There is an inability to detect and manage incidents that affect data security" it is collected that "There is NO procedure to detect and manage information security incidents or breaches.

IV. In relation to the potential risk scenario with code RDL.04 and description "Violation of the secrecy of communications" is states that "The staff has NOT formalized the commitment to confidentiality on the part of the organization.

10. That within the office there are sealed deposits to introduce

any document where personal data may work. that despite not

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

10/20

There should still be a formal and written procedure provided to employees for the destruction of supports and documents, the employees were transferred a Communiqué with the purpose of reinforcing the importance of diligence in the processing of personal data expressly stating instructions for the destruction of documentation.

11. That no audit was carried out with the previous consultant. Within the hiring of the consultant specialized in the protection of data is audited in the second year.

On January 28, 2020, TIPSA sends this Agency the following information and demonstrations:

1. That, having carried out the appropriate investigations, it has been possible to verify the following:

“-Of all the information received or known prior to the Incident related to compliance with data protection regulations data by GIEXPRESS and, as no type of data has been detected of anomaly on its part, it could not be glimpsed by TIPSA such lack of diligence on the part of the treatment manager.

...

-This is an isolated incident, no other employee has performed or is performing similar behavior.

-Regarding the degree of intentionality, none has been detected.

cause or special condition that could motivate the production of the reported facts.

-Similarly, no recurrence can be appreciated, as it is the first incident/non-compliance verified.”

2. That the security measures implemented prior to the incident, are among others:

“Prior to May 25, 2018, TIPSA carried out a process of adaptation to the RGPD in which it implemented a specific system of compliance with the aforementioned regulations, carrying out by the entity the identification, review and adequacy of character data processing staff.

As a result of this process, a documentary was prepared that forms the basis of the organization's Compliance System, composed, among others, by the following elements:

- Record of treatment activities carried out by TIPSA.
- Analysis of prior risks of each and every data processing carried out by TIPSA, and definition of technical security measures and organizations to apply.
- Model contracts to regularize the relationship with third parties that have access to data of a personality nature that is the responsibility of TIPSA.
- Models of confidentiality agreements and duty of secrecy to be signed with personnel with access to data (authorized personnel) and without access to data

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

C/ Jorge Juan, 6

28001 – Madrid

(unauthorized personnel), in which the obligations of confidentiality and secrecy, as well as data processing protocols personal.

-Information clauses drafted ad hoc to comply with the duty of transparency and information of each treatment.

-Specific protocols and procedures to guarantee, internally and externally, among others, the exercise and attention to the rights of interested; the notification and management of incidents and security violations; the contracting of third parties with access to data; authorization management and access control; data retention and secure destruction; the staff education and training.

-Assessment of the need to carry out Impact Assessments on the Data Protection (EIPD) of the treatments.

...

Prior to the knowledge of the incidence that occupies us the present report, TIPSA had implemented, among others, the following measures of security (organizational and technical) with respect to GIEXPRESS and all third parties with access to data on behalf of TIPSA:

-Establishment of an internal procedure to guarantee the signing of the corresponding treatment commission contract in the terms established by data protection legislation with suppliers with Data access.

-Contractual establishment of a communication protocol with the in charge of treatment to guarantee the exercise and attention to the rights of the interested parties, and the notification and management of incidents and

security breaches.

-Contractual establishment of the specific security measures to

implemented by third parties with access to data to guarantee the

confidentiality, integrity and availability of personal data.

-Contractual establishment of mechanisms for supervision, verification and

auditing of processing entrusted to third parties.

-Establishment of internal procedures to communicate and raise awareness

on the different instructions to be used in data processing

(from collection to destruction), both by staff

own and by third parties.

...”

3. That an action plan has been undertaken with a series of measures to be carried out

cape:

a. Measures of immediate application, among others:

“-Establishment of mechanisms for supervision, verification and

auditing of processing entrusted to third parties to

verify that they comply with the stipulations of the contract.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

12/20

-Review of the risk analysis carried out regarding the treatment

where the incident occurred, in order to document a

increase the probability and define new measures of

security based on the detected risk.

-Review of the clauses set forth in the order contract

of the treatment, in order to guarantee the correct fulfillment  
of the instructions provided by TIPSA and the adoption of the  
adequate security measures.

-Requirement to GIEXPRESS of subscription/renewal of the  
confidentiality commitments with all its employees  
(authorized personnel), in order to be formally notified  
and make them aware of the obligations of secrecy and  
confidentiality they have on the data of character  
staff, to comply with the corresponding security measures  
and the consequences of its non-compliance.

-Request and review of the agreements signed by GIEXPRESS,  
as person in charge of processing personal data  
responsibility of TIPSA, with those subcontractors  
affected by this claim, in order to verify that  
conform to the same conditions established in the contract  
of order of the treatment signed between TIPSA and GIEXPRESS."

a. Measures in the process of application, among others:

"-Process of digitalization of paper documents and use of  
portable devices (POA, tablets...) that have measures  
adequate security measures to ensure confidentiality,  
integrity and availability of the data housed in said  
devices.

-Establishment of mechanisms for supervision, verification and  
auditing those in charge of treatment to verify that everything  
their subcontractor complies with the instructions and,

especially, the security measures, arranged by TIPSA

in the treatment order contract signed between TIPSA and

the treatment manager.

-Review of training content in the field of

Data Protection, in order to assess whether they comply with the

entity's operations.

...

-Establishment of training accreditation mechanisms

in terms of data protection given to its staff by

those in charge of treatment.”

1. Provides a Record of Treatment Activities.

2. Provides analysis and risk management.

3. Provides an analysis of the need to carry out an EIPD with the conclusion of “...no

it is considered necessary to carry out an EIPD for not complying with two or

more criteria from the treatment list that require EIPD referred to in

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

C/ Jorge Juan, 6

28001 – Madrid

13/20

article 35.4 RGPD and for not meeting any of the other criteria

significantly analyzed, which makes it unlikely that the treatment

by its nature, scope, context or purposes entails a high risk for the

rights and freedoms of natural persons”

THIRD: In accordance with article 65 of the LOPDGDD, the Director of the

Spanish Agency for Data Protection agreed to admit the claim for processing

filed by the claimant against the respondent.

FOURTH: On 06/09/2020, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged

infringement of article 5.1.f) of the RGPD, typified in article 83.5.a) of the RGPD and

sanctioned in accordance with the provisions of article 58.2.b) of the RGPD.

FIFTH: Once the initiation agreement was notified, the claimant on 07/01/2020 submitted

brief of allegations stating in summary the following: that it has been introduced

explicitly the destruction of documents in the contract signed with the supplier;

Provides new internal communication and driver confidentiality commitment

involved and internal circular signed by the same; annual audit is planned

by the hired consultant; In addition, it is intended to unify the action protocol of

security incidents, meetings every two months to determine any possible

infringement and annual audit on data protection.

SIXTH: On 08/18/2020, a period of practice tests began,

remembering the following

- Consider reproduced for evidentiary purposes the claim filed by the

claimant and his documentation, the documents obtained and generated by the

Inspection Services that are part of file E/08137/2019.

- Consider reproduced for evidentiary purposes, the allegations to the agreement of

home filed by the respondent and the documentation that accompanies them.

SEVENTH: On 02/04/2021, a Resolution Proposal was issued in the sense that

by the Director of the Spanish Agency for Data Protection to sanction the

claimed for an infringement of article 5.1.f) of the RGPD, typified in article

83.5.a) of the RGPD, with a penalty of warning.

After the legally stipulated period, the respondent has not submitted a written

any allegation.



EIGHTH: Of the actions carried out in this proceeding, they have been

accredited the following:

#### PROVEN FACTS

FIRST: That on 05/07/2019 a technician from the claimant's Environment located a

dumped out of waste containers, including delivery notes

and package delivery documentation from the TIPSA company (a total of 212

folios) in which names, surnames, DNI and address of natural persons appear.

SECOND: Photographs of the containers with the garbage and a copy of the

the TIPSA delivery documentation containing personal data.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

14/20

THIRD: TIPSA in writing dated 07/12/2019, has indicated that its business model

lies in the creation of a network of freight forwarding agencies,

proceeding to sign contracts with existing agencies; contract is provided

agreement between TIPSA and the defendant dated 10/21/2004, as well as the

novation of the same on 05/01/2008.

FOURTH: The respondent in writing has indicated that once the incident became known,

after TIPSA's letter, it was understood that the event should be investigated, stating that:

“The carrier that caused the incident, at that time, was hired as

reinforcement given the increase in the volume of work in that period” and that “This entity

concluded that it was a human error due to lack of diligence, without the appearance of

bad faith or intention to harm the privacy of the data contained in said

documents and without deriving any economic benefit from such action for

the responsible carrier.

## FOUNDATIONS OF LAW

By virtue of the powers that article 58.2 of the RGPD recognizes to each control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD,

The Director of the Spanish Agency for Data Protection is competent to initiate and to solve this procedure.

Yo

Article 58.2.b) of the RGPD indicates:

II

"two. Each supervisory authority will have all of the following powers corrections listed below:

(...)

b) sanction any person responsible or in charge of the treatment with warning when the treatment operations have infringed the provided in this Regulation;

III

The facts claimed are specified in the discharge outside the containers of waste, of delivery notes and documentation of parcel delivery of the company TIPSA, a total of 212 pages, including the personal data of natural persons, conduct that violates data protection regulations, duty of confidentiality.

Such treatment could constitute an infringement of article 5,

Principles related to the treatment, of the RGPD that establishes that:

"1. The personal data will be:

(...)

f) treated in such a way as to ensure adequate security of the

personal data, including protection against unauthorized processing or against its loss, destruction or accidental damage, through the application of appropriate technical or organizational measures ("integrity and confidentiality").

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

15/20

(...)"

Article 5, Duty of confidentiality, of the new Organic Law 3/2018, of 5 December, Protection of Personal Data and guarantee of digital rights (hereinafter LOPDGDD), states that:

"1. Those responsible and in charge of data processing as well as all people who intervene in any phase of this will be subject to the duty of confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary of the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will remain even when the relationship of the obligor with the person in charge or person in charge had ended of the treatment".

IV

In the present case, the conduct of the defendant evidences the violation of the article 5.1.f) in relation to article 32.1 of the aforementioned regulation. As stated in the proven facts on 03/9/2020 an environmental technician from the City Council of

\*\*\*LOCATION.1 located a waste dump outside the garbage containers,

related to delivery notes and parcel delivery documentation of the company TIPSA, adding a total of 212 pages, in which names, surnames, DNI and address appear of natural persons.

The duty of confidentiality, previously the duty of secrecy, must understood that its purpose is to prevent leaks of data not consented to by their owners.

Therefore, this duty of confidentiality is an obligation that falls not only to the person in charge and in charge of the treatment but to everyone who intervenes in any phase of the treatment and complementary to the duty of professional secrecy.

In accordance with the provisions of article 5.1.f) of the RGPD, the personal data must be treated in a way that guarantees the security and confidentiality adequate, including the impossibility of unauthorized access or use of said data and the equipment used in the treatment ("principles of integrity and confidentiality").

Therefore, it constitutes a legitimate interest of the person in charge, the treatment of personal data to the extent strictly necessary and proportionate to ensure their safety (i.e. the ability to resist, at a given level of trust, to accidental events or illicit or malicious actions that compromise the availability, authenticity, integrity and confidentiality of data personal data stored or transmitted), which could include, preventing unauthorized access access to communications networks and the malicious distribution of codes, stop attacks and damage to computer and communication systems electronics.

It should be noted that the loss of confidentiality of the data subject treatment, etc., poses a risk to the rights and freedoms of people physical whose gravity and probability will depend on the nature, scope,

context and purposes of data processing. In order to maintain security and prevent that the treatment violates the provisions of the RGPD, the person in charge or the person in charge

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

16/20

they must evaluate the risks inherent to the treatment and apply measures to mitigate them.

These measures must guarantee an adequate level of security, including confidentiality, taking into account the state of the art and the cost of its application regarding the risks and the nature of the personal data that must be protect yourself. When assessing the risk in relation to data security, take into account those that derive from the processing of personal data, such as accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the communication or access is not authorized to said data, susceptible in particular to cause damages physical, material or immaterial, all to prevent damage from happening and a security breach may occur.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

17/20

It should be noted that TIPSA and the respondent maintain a contract of collaboration; before the request for information from the first, the respondent indicated that it was all due to human error.

Also the one claimed in his response to the informative request of the Agency stated that they had knowledge of the incident through the information provided by TIPSA and that the carrier causing the incident of security had been hired as reinforcement given the increased volume of work in the period in which the incident occurred and that the management of delivery notes and deliveries was at a time of technological adaptation and process of change of physical documentation to the use of mobile application, process that would end on 07/09/2019, at which time the documentation was completely dispensed with physical. It also indicated that they had a service provider for the periodic collection of documents using sealed containers, having transferred to employees information in order to reinforce the importance in diligence in the processing of personal data expressly appearing documentation destruction instructions.

The respondent has also provided a Record of Processing Activities and Risk analysis and management,

For its part, TIPSA, once the analysis and investigation of the incidence, has stated that it was an isolated incident and that it has not been detected intentionality that could motivate the events produced.

The person claimed by writing sent to this Agency has indicated having proceeded to adopt a series of measures, without prejudice to adopting and incorporating others, on its own initiative or those that this body may submit to it, among which finds the performance of an annual audit by the consultant in the field of data protection contracted by the company and that in the report that it has transferred has revealed a series of deficiencies that must be corrected with your advice.

At the same time and in order to prevent similar incidents from occurring, and

in a process of improving its regulatory compliance will carry out a series of actions, including unifying the protocol for action in the event of incidents of security and the protocol of action in the event of possible breaches or infractions in data protection in order to improve transparency and coherence internal in data processing; hold bi-monthly meetings to to determine and detect any possible violation of the protection of data; perform annual audits on data protection with the entity contracted to determine if future changes could justify another type of measures to be taken.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

18/20

On the other hand, the contract with the supplier has been modified explicitly introducing certain mention to the destruction of documents, to in order to record said end; confidentiality agreement of the autonomous carrier involved in the claimed security incident and the circular signed by him; workers have received new training in the matter to prevent events such as the one that occurred and that has adequate procedures in place of action in the destruction of documents, the incidence being a consequence of punctual error in the operation of said procedures, which have been reinforced to avoid events similar to the one produced.

v

Article 83.5 a) of the RGPD, considers that the infringement of “the principles basic for the treatment, including the conditions for the consent in accordance with

of articles 5, 6, 7 and 9” is punishable, in accordance with section 5 of the mentioned article 83 of the aforementioned GDPR, “with administrative fines of €20,000,000 maximum or, in the case of a company, an amount equivalent to 4% as maximum of the overall annual total turnover of the previous financial year, opting for the highest amount.

The LOPDGDD in its article 72 indicates: “Infringements considered very serious:

1. Based on the provisions of article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

suppose a substantial violation of the articles mentioned in that and, in

particularly the following:

a) The processing of personal data violating the principles and guarantees established in article 5 of Regulation (EU) 2016/679.

(...)

However, article 58.2 of the RGPD provides the following: “Each authority of control will have all the following corrective powers indicated below:

continuation:

(...)

b) sanction any person responsible or in charge of the treatment with warning when the processing operations have violated the provisions of this Regulation;

(...)

Therefore, the RGPD, without prejudice to the provisions of its article 83, contemplates in its article 58.2 b) the possibility of going to the warning to correct the processing of personal data that do not meet your expectations.

In the case at hand, the present sanctioning procedure has

It has been proven that the defendant violated the principle of confidentiality of the



data by enabling unauthorized access to them as a result of the

abandonment of the documents that contained them.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

19/20

In accordance with the evidence available to said conduct

constitutes by the claimed party the infringement of the provisions of article 5.1.f) of the

GDPR.

This infraction could be sanctioned with a warning in accordance with the

article 58.2.b) of the RGPD and consider that the administrative fine that could fall

in accordance with the provisions of article 83.5.b) of the RGPD could constitute a burden

for the defendant, in addition to the fact that there is no record of the commission of any previous infraction

in terms of data protection.

Likewise, it is necessary to point out that not correcting the incidents produced

in accordance with the provisions of the RGPD applying appropriate technical measures to the

risk presented by the treatment of the data, as a consequence of the destruction,

accidental or unlawful loss or alteration of personal data that has been

transmitted, stored or otherwise processed, or the communication or access is not

authorized to said data and that could cause physical damages,

material or immaterial, or to repeat the behavior revealed in the

claim and that is the cause of this procedure, as well as not informing this

AEPD of the rest of the measures adopted could give rise to the exercise of possible

actions before the person in charge of the treatment so that they are applied in a

take appropriate measures to ensure and not compromise confidentiality

of personal data and the right to privacy of individuals.

Therefore, in accordance with the applicable legislation and having assessed the criteria for graduation of sanctions whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE GIRONA INTEGRAL EXPRESS, S.L., with NIF B17770991, for an infringement of article 5.1.f) of the RGPD, typified in article 83.5 of the RGPD, a sanction of warning.

SECOND: NOTIFY this resolution to GIRONA INTEGRAL EXPRESS, S.L. with NIF B17770991.

In accordance with the provisions of article 50 of the LOPDGDD, the

This Resolution will be made public once it has been notified to the interested parties.

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 period of

month 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.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP, the firm resolution may be provisionally suspended in administrative proceedings if the interested party expresses his intention to file a contentious appeal-administrative. If this is the case, the interested party must formally communicate this made by writing to the Spanish Agency for Data Protection, introducing him to the agency [<https://sedeagpd.gob.es/sede-electronica-web/>], or through any of the other records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also must transfer to the Agency the documentation that proves the effective filing of the contentious-administrative appeal. If the Agency were not aware of the filing of the contentious-administrative appeal within two months from the day following the notification of this resolution, it would end the precautionary suspension.

Electronic Registration of  
through the  
Sea Spain Marti  
Director of the Spanish Data Protection Agency  
C/ Jorge Juan, 6  
28001 – Madrid  
[www.aepd.es](http://www.aepd.es)  
[sedeagpd.gob.es](https://sedeagpd.gob.es)