

File No: PS/00372/2021
IMI Reference: A56ID 122865- Case Register 128401

FINAL DECISION ON PENALTY PROCEEDINGS

From the actions taken by the Spanish Data Protection Agency and based on the following

BACKGROUND

FIRST: [REDACTED] (hereinafter the complainant) lodged a complaint with the Polish Data Protection Authority. The complaint is directed against GLOVOAPP23, S.. L. with VAT B66362906 ('GLOVOAPP'). The grounds on which the complaint is based are as follows:

Having discovered that his home was not within the scope of GLOVOAPP's riders (information which is only obtained once an account is opened and personal data entered), the complainant requested the deletion of his account and personal data, on two occasions with a difference of 5 days, but did not receive a reply. In addition, the forms available on the Glovo app for the revocation of consent are available only in Spanish, not in English or Polish.

In addition to the complaint, he provides:

— Copy of an email sent on 7 November 2019 at 0.10 hrs from *liveops.comms@glovoapp.com* to [REDACTED], with the following message: "*Thank you for contacting Glovo! We have just collected your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period*". This email responds to a message dated 6 November 2019 at 23: 10 in which it is claimed that the delivery area is too small.

— Copy of an email sent on 12 November 2019 at 8:56 hrs from *liveops.comms@glovoapp.com* to [REDACTED], with the following message: "*Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period*". This email responds to a message dated 12 November 2019 at 8: 56 hrs explaining that his requests are not being dealt with. The complainant gives notice that he has already notified the Data Protection Authority and expects his account to be deleted immediately.

— Copy of an email sent on 12 November 2019 at 9:43 hrs from the email *liveops.comms@glovoapp.com* to [REDACTED], with the following message: '*Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period*'. This email responds to a message dated 12 November 2019 at 8: 43 hrs explaining that a week ago was sent an email requesting the deletion of his account and received no reply, but received an information document. He also warned that he would notify the

data protection authority that he did not have a request form for deletion of data in Polish, only in Spanish.

— Copy of an email sent on 13 November 2019 at 19:39 hrs from the email liveops.comms@glovoapp.com to [REDACTED], with the following message: “Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period”. This email responds to a message dated 13 November 2019 at 18: 39 hrs requesting that his personal data should be immediately no longer processed and deleted from all databases. In addition, he requests the deletion of his account within two working days.

SECOND: On 27 April 2020, the Spanish Data Protection Agency (AEPD) received the complaint via 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. This complaint is forwarded to the AEPD 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 its cross-border nature and that this Agency is competent to act as lead supervisory authority, given that GLOVOAPP has its registered office and main establishment in Spain.

This Agency agreed, on 18 May 2020, to be the competent authority to act as lead supervisory authority (LSA), in accordance with Article 56 (1) GDPR, as regards the right of erasure. However, it proposed to reject the part concerning the forms, as its inspection services checked that the data protection forms are downloaded in the language of the city selected on the homepage, and consequently the Polish forms are available if a Polish city is chosen.

The proposing authority raised the possibility to give the complainant the possibility to submit evidence that the forms were only available in Spanish at the time of the submission of the complaint, as the findings of the AEPD contested the complainant’s complaint at the time the check was carried out (i.e. five months after the submission of the complaint). They commented that they would send a letter to the complainant requesting such a remedy, and that if they did not receive a reply within 7 days, they would accept the rejection of that part of the complaint.

On 11 August 2020, this Agency received an email from the Polish authority, informing that no reply had been received from the complainant, and that, as a result, the part of the complaint relating to the forms was dismissed, which was reduced to the issue related to the exercise of the right to erasure (Article 17 GDPR).

According to the information entered into the IMI system, pursuant to Article 60 of the GDPR, it acts as a ‘supervisory authority concerned’, in addition to the Polish data protection authority, the supervisory authorities of Portugal, Italy and France. All of them under Article 4 (22) GDPR, since data subjects residing in these Member States are likely to be substantially affected by the processing at issue in these proceedings.

THIRD: In accordance with Article 65 (4) of Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights (hereinafter LOPDGGDD), GLOVOAPP was informed of this complaint so that it could analyse it and inform this Agency within one month, of the measures taken to comply with the requirements laid down in the data protection legislation.

The request, which was carried out in accordance with the rules laid down in Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations ('LPACAP'), was recorded on 20 August 2020 as stated in the acknowledgement of receipt in the file.

On 18 September 2020, the Agency received a letter of reply stating:

- The origin of the incident lies in the fact that, contrary to what the complainant indicates, his personal data was not requested to be erased using the form provided for that purpose on the web portal, but by means of a chat with an agent of customer care service (SAC) in charge of management of orders and related incidents. Instead of using the various visible, clear and specific channels made available by the company, both on its website and in its application, to exercise his personal rights, i.e. the addresses *legal@glovoapp.com* and *gdpr@glovoapp.com*, as well as the different rights exercise forms published on the website and accessible in the application in the 'Contact' section, he requested the erasure of his data by means of an incorrect channel, not intended for this purpose.
- They state that their SAC assigns an agent responsible for answering users depending on the territory in which the user is located, in order to be able to reply in the same language as that in which the request is launched. In this case, the complainant was not assigned any city or territory since, as he had not placed an order via the app, he could not be located on the basis of the territory. This is why, in view of the fact that it was impossible to locate the user in a particular city, the system did not transmit the requests for erasure of data to any SAC actor, and the user received only the response that the SAC automatically generates before an agent responsible for responding to users is assigned.
- Following the transfer of the complaint, they have erased the complainant's personal data (clarify that they only had their email address, as he did not have any orders), and have contacted him to inform him of this, and of the retention of his data in a blocked state, inter alia, in order to defend themselves in complaints (they provided a copy of the email dated 16 September 2020). They explain that the reason for not having complied with his request was the use of an incorrect channel to exercise his right.
- In order to avoid such incidents occurring in the future, they have sent a reminder to all agents about the need to send to the Office of the Data Protection Officer all communications that may include a request for the exercise of rights, even if this request is hidden or not obvious. They have also reported to the SAC department the inconvenience related to the allocation of requests by users who have not placed orders or who have not indicated a country or address when registering in the app. As long as a technical solution to the problem is not found,



its staff shall monitor, manually and periodically, applications which have not been automatically assigned to any staff member.

- They also disagree with the fact, reported by the complainant, that forms are not available in their language, and also that it is necessary to open an account in order to know the geographical area of availability of service, since the coverage of mailings is accessible via a dedicated URL (<https://glovoapp.com/es/map> in Spain, for example).

FOURTH: On 11 December 2020, pursuant to Article 65 of the LOPDGDD, the complaint lodged by the complainant was declared admissible.

FIFTH: On 5 October 2020, the Director of the AEPD adopted a draft decision to discontinue the proceedings. Following the process set out in Article 60 GDPR, this draft decision was submitted via IMI on the same day and communicated to the concerned supervisory authorities that they had four weeks from that date to raise relevant and reasoned objections. Within the time limit set for that purpose, the Polish supervisory authority submitted its relevant and reasoned objections for the purposes of Article 60 of the GDPR, in the sense that it considered that there was no need to discontinue the proceedings but rather to analyse the case and issue a reprimand given that there had been an infringement of the GDPR. For its part, the Portuguese supervisory authority submitted its relevant and reasoned objections in the same sense, taking the view that GLOVOAPP should be penalised for an infringement of the GDPR.

SIXTH: On 3 September 2021, the Director of the AEPD adopted a revised draft decision initiating penalty proceedings. Following the process set out in Article 60 of the GDPR, this revised draft decision was transmitted via IMI on 6 September 2021 and the authorities concerned were informed that they had two weeks from that time to raise relevant and reasoned objections. Within the period for that purpose, the supervisory authorities concerned did not raise relevant and reasoned objections in that regard, so that all the supervisory authorities are deemed to agree with and are bound by that revised draft decision, in accordance with Article 60(6) GDPR.

SEVENTH: On 31 March 2022, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against GLOVOAPP, in accordance with Articles 63 and 64 of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations ('the LPACAP'), for the alleged infringement of Article 12 of the GDPR, in conjunction with Article 17 of the GDPR, as set out in Article 83 (5) of the GDPR.

The initial agreement was notified in accordance with the rules laid down in the LPACAP on 11 April 2022, as stated in the acknowledgement of receipt in the file.

EIGHT: On 19 April 2022, GLOVOAPP submitted a letter requesting an extension of the deadline for submitting arguments.

NINTH: On 21 April 2022, this Agency decided to extend the time limit to a maximum of five days, in accordance with Article 32 (1) of the LPACAP.

The extension agreement was notified to GLOVOAPP on the same day, as stated in the acknowledgement of receipt in the file.

TENTH: On 3 May 2022, this Agency received a letter in due time and form from GLOVOAPP in which it put forward arguments on the decision to initiate the procedure, in which it stated, in summary, that:

FIRST. ON GLOVO'S COMPLIANCE WITH PERSONAL DATA PROTECTION RIGHTS

First, GLOVOAPP refers to the statements presented in the letter dated 18 September 2020 concerning the events concerning the management of the right to erasure exercised by the former user of Glovo, a Polish national, through the chat managed by Glovo's Customer Care Service Department (SAC).

In those statements, GLOVOAPP understands that it was clear that, at no time, Glovo refused or hindered the exercise of the complainant's right to erasure for the purposes of Article 12.2 of the LOPDGDD, but rather that Glovo showed flagrant flexibility by deleting the complainant's personal data immediately after receiving the complaint from this Agency, despite not being exercised through the channels authorised for that purpose at that time (email addresses *legal@glovoapp.com* and *gdpr@glovoapp.com*).

GLOVOAPP also refers to the reasons why GLOVOAPP was unable to delete the complainant's personal data in due time (it was impossible to locate it in a specific territory or city because he had not placed an order via the platform and, consequently, it was impossible to assign his request to a specific agent of the SAC), which cannot, in any event, be understood as an intention on the part of Glovo not to comply with its duty of care to the complainant's right to erasure, for the purposes of Article 74 (c) of the LOPDGDD.

Moreover, GLOVOAPP notes that the complainant's right to erasure was immediately respected for the reasons already expressed in the letter of 18 September 2020, supplemented by a massive sending to all the agents who are members of the SAC reminding them of the need to immediately refer to the Data Protection Officer any exercise of rights that might be reached through the chat.

It is therefore clearly demonstrated that GLOVOAPP, as a controller, was already insured and continues to ensure in its internal policies the satisfaction of data subjects' rights, regardless of how they are exercised.

It states that GLOVOAPP regularly and constantly monitors all the channels it has contact with the user (web forms, app chat, email address, post, social media profiles, etc.) in such a way that, if a data protection right is exercised, it is properly respected.

It considers that evidence of this is that, since the complainant's complaint sent by this Agency, GLOVOAPP has not received any other complaint from the latter or from any other supervisory authority in the countries in which it operates for failure to comply with a right to data protection and, in particular, a right to erasure. And that all these actions by GLOVOAPP cannot be understood in any other way than as a clear willingness on the part of GLOVOAPP to comply with the rules on the protection of personal data.

In the light of the above, GLOVOAPP considers that the Agency should not finalise it with a reprimand, since the actions that have taken place cannot be understood as a clear intention to breach the data protection rules in the way that they do not wish to comply with the complainant's right to erasure, and the proceedings should be closed.

SECOND. — ON THE AGENCY'S DECISION ON THE CLOSURE OF THE PROCEEDINGS

GLOVOAPP makes express reference to the decision of 5 October 2020 by which the Director of the AEPD adopted a draft decision to discontinue these proceedings.

While the concerned supervisory authorities of Poland and Portugal raised objections to the draft decision, it is clear to GLOVOAPP that the draft decision is not adopted by the AEPD without considering that the actions and evidence obtained so far do not result in the existence of a breach or serious harm to the rights and interests of the complainant.

GLOVOAPP considers that the AEPD, as the lead supervisory authority in these proceedings, should have maintained the decision taken at the time, being the reprimand an unnecessary and inappropriate sanction for this case, since Glovo has never shown a willingness not to comply with the complainant's right to erasure, especially since it has shown clear and unequivocal flexibility by deleting his data immediately after receiving the complaint from the AEPD, despite the fact that this right has been exercised by a channel not authorised for this purpose.

In short, GLOVOAPP considers that Glovo has not failed to comply with data protection rules, which is why the closure of the proceedings is the most appropriate decision for this case.

THIRD. — NULLITY OF THE ADMINISTRATIVE ACT ON THE GROUND THAT THE INFORMATION NECESSARY TO ESTABLISH AN INFRINGEMENT IS LACKING

In addition, GLOVOAPP considers that in no case can Glovo's conduct be sanctioned in the form of a reprimand, for the reasons set out below.

3.1 Absence of subjective elements of the infringement. Nullity of penalty

GLOVOAPP takes the view that it is necessary, first of all, to examine whether or not the essential elements and conditions necessary for the imposition of a penalty in this case have been met.

Thus, the principles governing the administration's power to impose penalties will be, in general, those of administrative sanctioning law and, in particular, 'the principles of legality, criminality, liability, proportionality and non-participation'.

Law 40/2015 of 1 October 1992 on the Legal Regime for the Public Sector provides that an administrative offence is an action, understood in the broad sense of any action — or omission by persons seeking to produce a result — and which the Legislator itself has classified as an infringement.

In accordance with the above, in order to be faced with a personal data protection infringement, there must have been an intentional or negligent act or omission of any degree of negligence. What does this mean? That the person liable could, at the very least, have required different conduct.

Without wishing to subscribe to a compendium of sanctioning law, we can define subjective elements of the type such as the different degrees of voluntary nature or, at the very least, failure to comply with due diligence; deception is the clear manifestation of the voluntary nature of the typical action in the commission and mere negligence is the conduct that lacks the necessary care in complying with health obligations.

Thus, it is for the competent body to examine whether the conduct under examination is intentional or negligent, since such an assessment is essential in order to be able to impose a penalty, since they are constituent elements of the administrative offence.

The case-law that could be cited in support of the above statement would be almost unlimited, so we will only refer to the judgment of the National High Court of 13 October 2005, since it gives a detailed overview of the principles of penalties, their development and the evolution of the applicable case-law criteria.

Given that the judgment referred to is rather lengthy, and in order not to prolong us unnecessarily by transcribing verbatim the entire content of the judgment, we can only extract the paragraphs that we consider to be most representative:

'Fourth... the assessment of guilt in the conduct of the offender is a requirement which arises directly from the constitutional principles of legal certainty and legality, as regards the exercise of powers to impose penalties of any kind. The principle of guilt is a basic element in classifying a person's conduct as punishable, i.e. it is an essential element in any administrative offence (...)

Sixth (...) In summary, guilt must be as proven as the active or negligent conduct penalised, and that evidence must be extended not only to the facts determining liability but also, where appropriate, to those which qualify or aggravate the offence. (...)

It is precisely the analysis of guilt which distinguishes a system of strict liability, in which it is penalised solely on the basis of the result, from one based on the principle of fault.

GLOVOAPP therefore understands that it can be concluded that the agreement notified to GLOVOAPP ignores one of the essential elements when it comes to being able to impose a penalty (even in the form of a reprimand), such as the examination of guilt, it being fully demonstrated that GLOVOAPP did not at any time intentionally wish to disregard the complainant's right to erasure. The opposite is true. Glovo immediately drew attention to that right once it had been transferred by that agency.

GLOVOAPP therefore states that it must be borne in mind that the AEPD should have carried out this analysis and that, therefore, it cannot be established that Glovo intended to infringe the data protection legislation (in the way that it wished to hinder, prevent or not comply with the complainant's right to erasure), and that the assessment of that intention as an essential element of the administrative offence was disregarded. GLOVOAPP takes the view that the imposition of a penalty would be null and void.

3.2. The absence of evidence rebutting Glovo's presumption of innocence. Nullity of penalty

In this regard, it should be noted that, as it has been repeatedly pointed out by the case-law, the existence of conduct constituting an administrative offence is a prerequisite and inexcusable for the imposition of any administrative penalty. The administration cannot therefore penalise without sufficiently proving the guilt of the person penalised, that is to say, the existence of bad faith in its conduct. It is therefore clear that the administration bears the burden of proving the guilt of the person concerned, which must be proved by any of the means permitted under the law.

However, in the present case, GLOVOAPP is not aware that there is absolutely no evidence to support the rebuttal of the presumption of innocence which, within the administrative and sanctioning sphere, is fully applicable to relations between the administration and those administered, as has been recognised by countless judicial decisions in all hierarchical and territorial areas.

In this regard, for example, the judgment of the High Court of Justice of 10 June 1994 stated: *'(...) in the exercise of the power of the public authorities to impose penalties, the presumption of innocence of any person accused of an offence is, to the fullest extent possible, a presumption of innocence until proven guilty. This principle, incorporated in Article 24 of our Constitution, has the immediate procedural consequence of shifting the burden of proof to the accused, and in the case of the power to impose penalties, to the public administration. In adversarial proceedings, with the participation and hearing of the accused, it is for the defendant to provide, collect and produce the evidence, using common means to support the factual situation which it is claimed to be classified as an administrative offence. If no such evidentiary activity has taken place, it is clear that the account or description of the events by the authority or its staff does not give rise to a presumption of veracity which would oblige the accused to prove his innocence, thereby reversing the burden of proof'* (SSTS of 16 December 1986 and 26 December 1988)

Similarly, in relation to this lack of evidence and for the purposes of assessing what happened in the present case, the judgment of the Supreme Court of 26 December 1983 (RJ 1983\ 6418), which provided as follows: *'(...) In matters relating to penalties, it is not sufficient for the Administration to believe that a person has carried out certain facts in order to apply the penalty applicable to them. Rather, it is necessary to establish that he is indeed the author of those acts, and this requirement cannot be considered to have been complied with by two reports, which (...) are no longer a subjective assessment of the person who issued them and that, even if the person who issued them is enhanced by the status of the author, it cannot be the decisive factor that the Administration seeks, when the person concerned contradicts it in full detail, and when it relates to facts which, by their very nature, could have been easily and definitively proven or confirmed by the most varied means (...). In the area of penalties under administrative law, it is not appropriate to rely on reasonable grounds, or conscientious assessments, in order to establish an administrative offence, by imposing on the administration which accuses and penalises, under the presumption of innocence, the burden of proving the truth of the acts he accuses, and that those facts are imputable to the accused person, given that the presumption of innocence referred to above, now enshrined in Article 24 of the Constitution, can only be rebutted by proof of guilt'* SS of 16 February, 23 March and 28

September 1982 (RJ 1982/968, RJ 1982/2324 and RJ 1982/5513), the legality of administrative penalties is conditioned by the nature of the offence and the penalty and by the conclusive and unequivocal proof that the person penalised is responsible for it, recalling the Chamber's Supreme Court of 23 December 1981 (RJ 1981/5453) that the prosecution, in particular, of an administrative decision finalising corrective or penalty proceedings must be based on the analysis of the facts or act challenged, of its nature and scope. in order to determine and see whether or not the administrative offence pursued can be subsumed in one of the cases, the types of administrative offence provided for in the legislation which serves as the basis for estimating the infringement sought and, where appropriate, punished, a prosecution which must be carried out on the basis of a purely legal criterion, since the classification of the administrative offence is not a discretionary power of the administration or of the sanctioning authority, but rather a legal activity which requires, as an objective condition, the offence to be included in the predetermined legal category as a fault, the liability for an administrative offence cannot be resolved on the basis of mere presumptions, indicia or conjecture, but on the basis of the reality of facts that are fully established and proven (...).'

In those circumstances, it is clear that the Agreement should be required to go beyond the mere reference to the legal provisions of the LOPDGDD to which reference has been made above. In the present case, GLOVOAPP takes the view that the AEPD confines itself to reviewing the background to the file in the Agreement, but, as has been demonstrated, it can in no way be said that we are faced with a clearly intentional infringement of the data protection legislation by Glovo, especially if, as has been shown in the facts, the complainant's right to erasure was clearly respected.

In the view of GLOVOAPP, the main objective of the penalty proceedings must be to break the presumption of innocence enjoyed by any person required by seeking the intentional element in his action, the subjective element of the administrative offence by means of an evidentiary activity that can be considered sufficient.

However, GLOVOAPP considers that in the present case there is no real incriminating evidence in the initiation of proceedings to suggest that GLOVOAPP's conduct is culpable.

In the light of all the above arguments, GLOVOAPP asked the AEPD to withdraw the agreement imposing a penalty imposed on GLOVOAPP, on the grounds that it wished to be imposed with a total absence of evidence of guilt and, consequently, in breach of the fundamental right to the presumption of innocence enshrined in the Spanish Constitution.

3.3. Absence of guilt. Nullity of penalty

In order to prove the absence of guilt, GLOVOAPP refers, with regard to the invocation of the principle of guilt, that the Constitutional Court has established as one of the basic pillars for the interpretation of administrative sanctioning law that the principles and guarantees present in the area of criminal law are applicable, with certain nuances, in the exercise of any power to impose penalties on the part of the public administration (STC 76/1990 of 26 April 2007).

In its judgment of 10 February 1986, the Supreme Court stated that *'the exercise of the power to impose penalties, whatever its manifestations, must be consistent with the constitutional principles and requirements governing the criminal legal system as a whole, and, whatever the sphere in which the State's punitive power, the courts, or the field in which it occurs, are subject to the same principles, the observance of which legitimises the imposition of penalties and penalties. therefore, administrative offences must, in order to be punishable or punished, be typical, that is to say, provided for as such by previous legal rules, which are unlawful, that is to say, damage to a legal asset provided for by law, and culpable, attributable to an perpetrator on the basis of willful misconduct or fault, in order to ensure, in his assessment, the balance between the public interest and the guarantee of individuals, which is the key to the rule of law'*.

In the specific case, at no time has GLOVOAPP failed to comply with the data protection rules, and GLOVOAPP considers that it has fulfilled all its obligations in a religious manner. There has been no intention to infringe, quite the contrary.

GLOVOAPP considers that it has demonstrated to the AEPD its willingness to comply with the rules on the protection of personal data by immediately deleting the complainant's data once the complaint has been forwarded by the AEPD and ensuring that users' rights are fully satisfied at all times regardless of the channel they are exercised.

For all the above arguments, GLOVOAPP considers that there is a complete absence of evidence of guilt and, consequently, a violation of the fundamental right to the presumption of innocence enshrined in the Spanish Constitution.

3.4. Absence of the principles of criminality and presumption of innocence. Nullity of penalty

GLOVOAPP considers it necessary to highlight the non-existence of the conduct found to constitute an infringement and for which it is penalised in administrative proceedings.

This should have led the AEPD to close the penalty proceedings against GLOVOAPP (decision already taken by the AEPD in its draft decision of 5 October 2020), since otherwise there would be a flagrant breach of the principle of criminality resulting from the applicable legislation.

It has already been stated, in principle, that the legal system protects those involved in penalty proceedings by requiring that the administrative bodies responsible for the initiation of penalty proceedings consider as infringements only conduct that adequately falls within the definitions that explicitly establish rules with legal status. Thus, the first paragraph of Article 129 of Law 40/2015 provides as follows: **'Article 27. Principle of criminality. 1. Administrative offences are only infringements of the legal order provided for as such by a law, without prejudice to the provisions of Title XI of Law 7/1985 of 2 April 1992 for the Local Government'** (emphasis added and bold).'

In close connection with that provision, Law 40/2015 provides that the starting point for any action aimed at establishing liability for the commission of administrative offences must be to consider that, unless it is established otherwise, the person concerned has not committed the types declared as such.



As mentioned above, this is known as the principle of the presumption of innocence, which is fully consistent with the fact that the administration is obliged to carry out the investigative activity in order to verify whether specific conduct is subsumed into a type of infringement. Thus, with regard to the presumption of innocence, Law 39/2015 provides that that principle also applies to penalty proceedings.

With regard to the importance of compliance with the principle of criminality in the administrative procedure, the judgment of the Supreme Court of 2 June 2010, Chamber for Contentious Administrative Proceedings, Section 4, stated, and reproduced in extensive and consolidated legal literature, the following: *'The principle of criminality, the most important of those on which the right to impose an administrative penalty is based, requires, at the very least, a perfect match between the act and the final act as a breach, such as the objective and personal circumstances which determine the illegality, in order to establish precisely the conduct of the person concerned at the definitive rate by the provision deemed to have been breached (judgments of 25 March 1977, 13 May and 22 December 1986). Judgments of the Tribunal Supremo (Supreme Court) of 12 February.'*

As regards the principle of the presumption of innocence in the context of administrative powers to impose penalties, the case-law has also been unequivocal in that it requires administrative bodies to comply strictly with and subject to it. Thus, from an early stage — and settled case-law — the Constitutional Court has consistently held that the principle of the presumption of innocence fully subjects the power to impose administrative penalties.

As an example, reference may be made — for example — to Judgment of the Constitutional Court 13/1982 of 1 April 2007, which was expressed verbatim as follows: *'(...) the presumption of innocence is no longer a general principle of the right to be informed by judicial activity ("in dubio pro reo") in order to become a fundamental right which is binding on all public authorities and which is applicable immediately, as the Court has stated in numerous judgments.... The right to the presumption of innocence cannot be understood as being limited to the strict scope of prosecution of allegedly criminal conduct, but must also be understood as leading to the adoption of any decision, whether administrative or judicial, which is based on the status or conduct of the persons and which results in a penalty for them or limiting their rights.'*

In greater detail, the Supreme Court has also enshrined in its judicial activity the application of the principle of the presumption of innocence. Thus, by judgment of 28 February 1994, Chamber for Contentious Administrative Proceedings, Section 7, the High Court held: *'From a broad perspective, the identity of the principles of administrative sanctioning law with the power to impose criminal penalties is limited to the following general doctrines: the principle of legality (there is no administrative offence or penalty without any prior law determining them), the principle of typical unfairness (specific delimitation of the conduct to be criticised for the purposes of the penalty), the principle of 'nulla punición sine culpa' (the existence of intent or fault on the part of the perpetrator of the offence subject to the condition of a penalty) and, finally, with obvious significance in the present case, the principle of full proof of the reality of the impugned conduct, the expression of which in the constitutional principle of the presumption of innocence is clear, and which is sufficient to prove the actual performance by the accused of the*

impugned act or omission, with strict application of the right to impose administrative penalties'.

In view of the importance which the legal system attaches to the principles of criminality and the presumption of innocence in the context of the administration's power to impose penalties, and given the extensive acceptance in the case-law of the obligation to apply those principles to the administrative penalty procedure, all of the foregoing must be compared immediately with what happened in the present proceedings.

In the light of the above, GLOVOAPP considers that it has been duly demonstrated that it has always acted in good faith, applying the utmost effort to comply with data protection rules in the belief that it is lawful, as this is its requirement as a controller of the personal data of data subjects and with the aim of never jeopardising their rights and freedoms. There is therefore no clear 'intent' in failing to comply with the legislation in force, since it took all the necessary and appropriate actions to comply with the rules and has prudently aligned its actions with the law.

ELEVENTH: On 9 May 2022, the body conducting the penalty proceedings issued a proposal for a resolution, in which it proposed that the Director of the AEPD issue a reprimand to GLOVOAPP23, S. L., VAT B66362906, for an infringement of Article 12 of the GDPR, as set out in Article 83 (5) of the GDPR.

The proposal for a resolution was notified in accordance with the rules laid down in the LPACAP on 18 May 2022, as stated in the acknowledgement of receipt in the file.

TWELFTH: After the deadline for this purpose, we have not received any comments from GLOVOAPP on the above-mentioned proposal for a resolution.

The actions taken in these proceedings and the documentation contained in the file have shown the following:

PROVEN FACTS

FIRST: On 7 November 2019 at 0:10 hrs an email was sent from liveops.comms@glovoapp.com to [REDACTED] with the following message: *'Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period.'* This email responds to a message dated 6 November 2019 at 23:10 in which it is claimed that the delivery area is too small.

SECOND: On 12 November 2019 at 8:56 hrs an email was sent from liveops.comms@glovoapp.com to [REDACTED] with the following message: *'Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period.'* This email responds to a message dated 12 November 2019 at 8:56 hrs explaining that his requests are not being dealt with. The complainant notes that he had already notified the Data Protection Authority and he expects his account to be deleted immediately.

THIRD: On 12 November 2019 at 9:43 hrs an email was sent from *liveops.comms@glovoapp.com* to [REDACTED] with the following message: *'Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period'*. This email responds to a message dated 12 November 2019 at 8: 43 hrs explaining that a week ago he sent an email requesting the deletion of his account and received no reply, but received an information document. He also warned that he would notify the data protection authority that they did not have a request form for deletion of data in Polish, only in Spanish.

FOURTH: On 13 November 2019 at 19:39 hrs an email was sent from *liveops.comms@glovoapp.com* to [REDACTED] with the following message: *'Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period'*. This email responds to a message dated 13 November 2019 at 18: 39 hrs requesting that his personal data be immediately no longer processed and deleted from all databases. In addition, he requests the deletion of his account within two working days.

FIFTH: The Client Care Service (SAC) of GLOVOAPP allocates a user response agent depending on the territory in which the user is located, in order to be able to respond in the same language as the one in which the request is launched. In this case, the complainant was not assigned any city or territory, as he had not placed an order through the app and could not be located on the basis of the territory. This is why, since it was impossible to locate the user in a particular city, the system did not transmit the data deletion requests to any SAC actor, and the user received only the response that the SAC automatically generates before a user response agent is assigned.

SIXTH: Following the transfer of the complaint, GLOVOAPP has deleted the complainant's personal data (although they only had his email address, as he did not make any order), and have contacted him to inform him of this, and of the retention of his data in a blocked state, inter alia, to defend himself in complaints (by email dated 16 September 2020).

SEVENTH: GLOVOAPP has sent a reminder to all actors on the need to send to the Office of the Data Protection Officer all communications that may include a request to exercise rights, even if this request is hidden or not obvious. It has also reported to the department responsible for the SAC the inconvenience related to the allocation of requests by users who have not placed orders or who have not indicated a country or address when registering in the app. As long as a technical solution to the problem is not found, its officers will check, manually and regularly, requests that have not been automatically assigned to any actor.

LEGAL GROUNDS

I

Competence and applicable law

In accordance with the powers conferred on each supervisory authority by Article 58 (2) of Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)), and in accordance with Articles 47 and 48.1 of Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter LOPDGDD), the Director of the Spanish Data Protection Agency is responsible for initiating and deciding on this procedure.

In addition, Article 63(2) of the LOPDGDD provides that: *“The procedures handled by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, of this organic law, by the regulatory provisions dictated in their development and, insofar as they are not contradicted, alternatively, by the general rules on administrative procedures”*.

II Preliminary remarks

In the present case, in accordance with Article 4 (1) of the GDPR, there is a processing of personal data, since GLOVOAPP collects and stores, as a minimum, the electronic mail of natural persons, among other processing operations.

GLOVOAPP carries out this activity in its capacity as controller, since it is the controller who determines the purposes and means of that activity, pursuant to Article 4 (7) of the GDPR.

The GDPR provides, in Article 56 (1), for cases of cross-border processing, as provided for in Article 4 (23) thereof, in relation to the competence of the lead supervisory authority, that, without prejudice to Article 55, the supervisory authority of the main establishment or the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure set out in Article 60. In the case under consideration, as explained above, GLOVOAPP has its main establishment in Spain, so the Spanish Data Protection Agency is competent to act as the lead supervisory authority.

The right to erasure of personal data is regulated by Articles 17 of the GDPR and Article 15 of the LOPDGDD, while the way in which these rights are to be respected is regulated in Article 12 GDPR.

III Allegations

With regard to the allegations in response to the decision to initiate the present penalty proceedings, we will respond to them in the order set out by GLOVOAPP:

FIRST. ON GLOVO'S COMPLIANCE WITH PERSONAL DATA PROTECTION RIGHTS

GLOVOAPP understands that it became apparent that at no time did it deny or impede the exercise of the complainant's right to erasure for the purposes of Article 12.2 of the LOPDGDD, but rather showed flagrant flexibility by deleting the complainant's personal data immediately after receiving the complaint from this Agency, despite not being

exercised through the channels authorised for that purpose at that time (email addresses legal@glovoapp.com and gdpr@glovoapp.com).

In addition, it refers to the reasons why it was unable to delete the complainant's personal data in due time (it was impossible to locate it in a specific territory or city because it had not placed an order via the platform and, consequently, it was impossible to assign its request to a specific agent of the SAC), which cannot in any event be understood as an intention on the part of GLOVOAPP not to comply with its duty of care for the right of deletion exercised by the complainant, for the purposes of Article 74 (c) of the LOPDGDD.

Moreover, GLOVOAPP notes that the complainant's right to erasure was immediately respected for the reasons already expressed in the letter of 18 September 2020, supplemented by a massive sending to all the agents who are members of the SAC reminding them of the need to immediately refer to the Data Protection Officer any exercise of rights that might be reached through the chat.

It is therefore clearly demonstrated that GLOVOAPP, as a controller, was already insured and continues to ensure in its internal policies the satisfaction of data subjects' rights, regardless of how they are exercised.

In that regard, the Agency would like to point out that it was precisely not 'ensured' that the rights of data subjects would be satisfied, irrespective of the way in which they are exercised, since the complainant requested the deletion of their data via a channel which was certainly different from that provided for by GLOVOAPP, which is why the company was unable to comply with it correctly. This was, as the company acknowledges, due to the fact that the complainant had not placed an order, so that it could not be allocated a specific territory or city, which caused it not to be assigned a specific agent of the SAC to that request.

Although it is true that, after the complaint was forwarded by this Agency, GLOVOAPP has duly complied with the complainant's request, which is positively assessed by this Agency, the fact remains that the complainant's request was not complied with within the time limit laid down by the GDPR.

GLOVOAPP also maintains that it regularly and constantly monitors all the channels with which it has contact with the user (web forms, app chat, email address, post, social media profiles, etc.) so that, if a data protection right is exercised, it is properly respected.

This is demonstrated by the fact that, since the complainant's complaint sent by this Agency, GLOVOAPP has not received any other complaint from the latter or from any other supervisory authority in the countries in which it operates for failure to comply with a right to data protection and, in particular, a right to erasure.

However, this Agency would like to stress that the fact that no other complaint has been received from any supervisory authority does not constitute evidence that it 'monitors regularly and constantly all the channels with which it has contact with the user (...) in such a way that, if a data protection right is exercised, it is properly respected'.

In any event, it is clear that, irrespective of the action taken by GLOVOAPP after the facts at issue in these proceedings, at the time when the complainant made his request to delete his data, this monitoring was not being carried out or was not being carried out correctly, given that his right was not properly respected.

Finally, GLOVOAPP considers that the Agency is finalising it with a reprimand, but the actions that have taken place cannot be understood as a clear intention to breach the data protection rules in the way that they do not wish to comply with the complainant's right to erasure, and that they should be closed.

In this regard, the Agency does not consider that there was a clear intention to breach the data protection rules, but that GLOVOAPP acted negligently by failing to provide for an internal mechanism to deal with requests concerning the exercise of rights under the legislation on the protection of personal data received via channels other than those initially provided for. In particular, in cases where the system could not assign a given SAC agent, as a specific city or territory cannot be assigned to the user, as was the case in the present case.

In the light of the above, the present claim is rejected.

SECOND. — ON THE AGENCY'S DECISION ON THE CLOSURE OF THE PROCEEDINGS

GLOVOAPP makes express reference to the decision of 5 October 2020 by which the Director of the AEPD adopted a draft decision to discontinue these proceedings.

While the concerned supervisory authorities of Poland and Portugal raised objections to the draft decision, it is clear to GLOVOAPP that the draft decision is not adopted by the AEPD without considering that the actions and evidence obtained so far do not result in the existence of a breach or serious harm to the rights and interests of the complainant.

GLOVOAPP considers that the AEPD, as the lead supervisory authority in these proceedings, should have maintained the decision taken at the time, the reprimand being an unnecessary and inappropriate sanction for this case, since Glovo has never shown a willingness not to comply with the complainant's right to erasure, especially since it has shown clear and unequivocal flexibility by deleting his data immediately after receiving the complaint from the AEPD, despite the fact that this right has been exercised by a channel not authorised for this purpose.

In this respect, the Agency would like to point out that the mechanism that Article 60 GDPR obliges the lead authority, in the case of cross-border processing, to take a unanimous decision together with the other authorities concerned. It is precisely envisaged that a new decision will be reached in which all supervisory authorities agree, either by means of a draft decision or a revised draft decision.

In this regard, the Spanish Agency initially proposed to the other authorities that the proceedings be discontinued by means of the aforementioned draft decision to discontinue the proceedings, but relevant and reasoned objections were raised which led this Agency to reconsider its initial interpretation, reaching an agreement with the

other authorities on the assessment of the existence of an infringement on the part of GLOVOAPP, without being obliged at any time to maintain its initial position.

On the basis of the above, the present claim is rejected.

THIRD. — NULLITY OF THE ADMINISTRATIVE ACT ON THE GROUND THAT THE INFORMATION NECESSARY TO ESTABLISH AN INFRINGEMENT IS LACKING

GLOVOAPP considers that under no circumstances can their conduct be sanctioned in the form of a reprimand, for the reasons set out below.

3.1 Absence of subjective elements of the infringement. Nullity of penalty

GLOVOAPP considers that the existence of intentional or negligent action in the present case has not been analysed in order to be able to impose a penalty in the present case. In other words, the existence of the subjective element (guilt) required by Law 40/2015 in order to establish the existence of an administrative offence has not been analysed.

Stresses GLOVOAPP that it has been proven that it has never intentionally wanted to disregard the complainant's right of withdrawal. The opposite is true. It has immediately taken this right into account once it has been transferred by this Agency.

GLOVOAPP therefore states that it must be borne in mind that the AEPD should have carried out this analysis and that, therefore, it cannot be established that Glovo intended to infringe the data protection legislation (in the way that it wished to hinder, prevent or not comply with the complainant's right to erasure), and that the assessment of that intention as an essential element of the administrative offence was disregarded. GLOVOAPP takes the view that the imposition of a penalty would be null and void.

In this regard, the Agency repeats what has been stated above, to the effect that we do not consider that there would have been a clear intention to breach the data protection rules, but that GLOVOAPP acted negligently by failing to provide for an internal mechanism to deal with requests concerning the exercise of rights under the legislation on the protection of personal data received by channels other than those initially provided for. In particular, in cases where the system could not assign a given SAC agent, as a specific city or territory cannot be assigned to the user, as was the case in the present case.

On the basis of the above, the present claim is rejected.

3.2. The absence of evidence rebutting Glovo's presumption of innocence. Nullity of penalty

GLOVOAPP submits that the administration bears the burden of proving the guilt of the person concerned, which must be proved by any of the means admitted in law.

And that, in the present case, it is not apparent that there is absolutely any evidence capable of rebutting the presumption of innocence which, within the administrative and sanctioning sphere, is fully applicable to relations between the administration and those

administered, as has been recognised by countless judicial decisions in all hierarchical and territorial areas.

In the present case, GLOVOAPP takes the view that the AEPD confines itself to reviewing the background to the file in the Agreement, but in no way can it be said that we are faced with a clearly intentional infringement of data protection rules by Glovo, especially if, as has been shown in the facts, the complainant's right to erasure was clearly respected.

GLOVOAPP considers that in the present case there is no real incriminating evidence at the time of that initiation of proceedings to suggest that there is guilt in GLOVOAPP's conduct.

In this regard, the Agency stresses that it does not understand that there was a clear intention to breach the data protection rules, but considers that GLOVOAPP acted negligently by failing to provide for an internal mechanism to deal with requests concerning the exercise of rights under the legislation on the protection of personal data received by channels other than those initially provided for. In particular, in cases where the system could not assign a given SAC agent, as a specific city or territory cannot be assigned to the user, as was the case in the present case.

As regards the evidence to that effect, GLOVOAPP stated in its reply to the transfer of the complaint and in its written observations on the decision to initiate the penalty proceedings that the request to delete the complainant's personal data had not been complied with, since it had not been possible to assign it into a specific SAC agent, since it had not placed an order and had not been assigned a specific city or territory. It was this situation that led to the failure to comply with the request made. And that, after becoming aware of the complaint, GLOVOAPP took measures to prevent this type of situation from recurring in the future (which has been positively assessed and it has been decided to replace a penalty in the form of a fine for issuing a reprimand, under the terms of the GDPR).

On the basis of the above, the present claim is rejected.

3.3. Absence of guilt. Nullity of penalty

GLOVOAPP insisted that, in the specific case, at no time the data protection legislation had been omitted or infringed, GLOVOAPP considered that it had fulfilled all its obligations in a religious manner. There has been no intention to infringe, quite the contrary.

GLOVOAPP considers that it has demonstrated to the AEPD its willingness to comply with the rules on the protection of personal data by immediately deleting the complainant's data once the complaint has been forwarded by the AEPD and ensuring that users' rights are fully satisfied at all times regardless of the channel they are exercised.

For all the above arguments, GLOVOAPP considers that there is a complete absence of evidence of guilt and, consequently, a violation of the fundamental right to the presumption of innocence enshrined in the Spanish Constitution.

In this regard, the Agency stresses that it does not consider that there was a clear intention to breach the data protection rules, but that GLOVOAPP acted negligently by failing to provide for an internal mechanism to deal with requests concerning the exercise of rights under the legislation on the protection of personal data received via channels other than those initially provided for. In particular, in cases where the system could not assign a given SAC agent, as a specific city or territory cannot be assigned to the user, as was the case in the present case. It therefore considers that there is sufficient evidence to show that GLOVOAPP acted negligently, which determines the existence of that infringement.

On the basis of the above, the present claim is rejected.

3.4. Absence of the principles of criminality and presumption of innocence. Nullity of penalty

GLOVOAPP points to the importance that the legal system attaches to the principles of criminality and the presumption of innocence in the context of the administration's power to impose penalties, and the extensive acceptance in the case-law of the obligation to apply those principles to the administrative penalty procedure, which must be compared with what happened in the present proceedings.

GLOVOAPP considers that it has been duly demonstrated that it has always acted in good faith, making every effort to comply with data protection rules in the belief that it is lawful, since it is its requirement as a controller of the personal data of data subjects and with a view to never jeopardising their rights and freedoms. There is therefore no clear 'intent' in failing to comply with the legislation in force, since it took all the necessary and appropriate actions to comply with the rules and has prudently aligned its actions with the law.

In this regard, the Agency stresses that it does not consider that there was a clear intention to breach the data protection rules, but that GLOVOAPP acted negligently by failing to provide for an internal mechanism to deal with requests concerning the exercise of rights under the legislation on the protection of personal data received via channels other than those initially provided for. In particular, in cases where the system could not assign a given SAC agent, as a specific city or territory cannot be assigned to the user, as was the case in the present case. It therefore considers that there is sufficient evidence to show that GLOVOAPP acted negligently, which determines the existence of that infringement.

On the basis of the above, the present claim is rejected.

IV

Right to erasure

Article 17 '*right of erasure ('right to be forgotten')*' of the GDPR provides that:

'1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have

the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2) and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase such data, the controller, taking account of available technology and the cost of the implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any link to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) and (3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims’.

Article 15 ‘Right of erasure’ of the Spanish LOPDGDD provides that:

'1. The right to erasure shall be exercised in accordance with the provisions of Article 17 of Regulation (EU) 2016/679.

2. When such erasure derives from the exercise of the right to object pursuant to article 21.2 of Regulation (EU) 2016/679, the controller may preserve the necessary data subject's identification data in order to prevent future processing for direct marketing purposes.'

In the present case, it is common ground that the complainant had requested GLOVOAPP to delete his personal data on at least four occasions.

V

Modalities for the exercise of the rights of the data subject

Article 12 '*Transparent information, communication and modalities for the exercise of the rights of the data subject*' of the GDPR states that:

'1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:



(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

(...)”.

Article 12 ‘General provisions on the exercise of rights’ of the Spanish LOPDGDD provides that:

‘1. The rights established in Articles 15 to 22 of Regulation (EU) 2016/679 may be exercised directly or through a legal or voluntary representative.

2. The controller shall be obliged to inform the data subject about the means available to him or her to exercise his or her rights. Such means shall be easily accessible by the data subject. The exercise of the right may not be denied on the sole ground that the data subject chooses a different means

3. The processor may process, on behalf of the controller, any request submitted by the data subjects to exercise their rights if this is established in the binding contract or legal act.

4. The evidence of compliance with the duty to respond to the request for the exercise of rights submitted by the data subject shall be the responsibility of the controller.

5. Where the laws applicable to certain processing establish a special regime that affects the exercise of the rights provided for in Chapter III of Regulation (EU) 2016/679, the provisions of those laws shall apply.

6. In any case, the holders of the parental authority may exercise in the name and on behalf of minors under fourteen years old the rights of access, rectification, cancellation, opposition and any other rights to which they may be entitled in the context of this organic law.

7. Any actions carried out by the controller to address requests to exercise these rights shall be free of charge, notwithstanding the provisions of articles 12.5 and 15.3 of Regulation (EU) 2016/679 and paragraphs 3 and 4 of article 13 of this organic law.’

In the present case, it is common ground that the complainant requested the deletion of his account and personal data on at least four occasions. The last of these on 13 November 2019. However, it was only on 16 September 2020 that GLOVOAPP confirmed to the complainant that it duly complied with that request, after having received the transmission of the aforementioned complaint from the Agency.

Although the complainant had not used the form for that purpose, he had contacted a customer service agent via a chat and had received an automatic reply from the undertaking to reply to it within 24 hours.

Indeed, it is the responsibility of the controller to ensure the satisfaction of data subjects' rights in general and, in particular, to comply with any requirements of the GDPR in relation to these rights. The accountability principle, in line with Article 5 (2) GDPR, implies that the controller must adapt its internal processes to comply with its regulatory obligations, in line with the organisation and processing of personal data it carries out. In addition, the controller must demonstrate that the solutions adopted comply with the requirements of the regulations.

In this context, the controller can and should have mechanisms that allow for the exercise of each of the rights in a simple way for data subjects and to give them full satisfaction in the shortest possible time. The controller should also demonstrate flexibility in the interaction with the data subject on a specific application, regardless of its internal policy. The fact that the request was made by means of an alternative to the mechanisms put in place by the undertaking should not be a reason not to comply with it.

Therefore, on the basis of the evidence available, the known facts are considered to constitute an infringement, attributable to GLOVOAPP, of Article 12 GDPR, read in conjunction with Article 17 GDPR.

VI

Sanction of the infringement of Article 12 GDPR

The infringement of Article 12 of the GDPR entails the commission of the infringements referred to in Article 83 (5) of the GDPR, which, under the heading '*General conditions for the imposition of administrative fines*', provides:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(...)

(b) the data subjects' rights pursuant to Articles 12 to 22; (...)

In that regard, Article 71 ('Infringements') of the Spanish LOPDGDD provides that:

'The actions and behaviours referred to in sections 4, 5 and 6 of Regulation (EU) 2016/679, as well as those which are contrary to this organic law, shall constitute infringements.'

For the purposes of the limitation period, Article 74 '*Minor infringements*' of the Spanish LOPDGDD states:

'In accordance with sections 4 and 5 of article 83 of Regulation (EU) 2016/679, any infringement consisting on merely formal lack of compliance with the provisions

mentioned therein, especially the ones listed below, shall be considered a minor infringement and its limitation period shall be one year:

(...)

(c) Failing to attend to the requirements to exercise any of the rights established by articles 15 to 22 of Regulation (EU) 2016/679, unless this results from the implementation of article 7.2.k) of this organic law’.

VII

Sanction for the infringement of Article 12 GDPR

Without prejudice to Article 83 of the GDPR, Article 58 (2) (b) of the GDPR provides as follows:

‘Each supervisory authority shall have all of the following corrective powers:

(...)

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; (...)’

Recital 148 of the GDPR states:

‘In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor..’

In accordance with the evidence available, the infringement in question is considered to be minor for the purposes of Article 83 (2) of the GDPR, given that in the present case it was a specific case, as a result of a one-off error (of which there are no similar records in this Agency), which would have already been corrected, which makes it possible to consider a reduction in fault in the facts, and it is therefore considered to be lawful not to impose a penalty consisting of an administrative fine and to replace it by issuing a reprimand.

Therefore, in accordance with the applicable legislation and assessing the criteria for graduation of penalties established, the Director of the Spanish Data Protection Agency DECIDES TO:

FIRST: Issue GLOVOAPP23, S.. L., with VAT B66362906, for an infringement of Article 12 of the GDPR, as set out in Article 83 (5) of the GDPR, a reprimand.

SECOND: Notify this resolution to GLOVOAPP23, S.L.

In accordance with Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

In accordance with Article 48.6 of the LOPDGDD, and in accordance with Article 123 of the LPACAP, interested parties may, by way of option, lodge an appeal against this decision with the Director of the Spanish Data Protection Agency within one month of the day following notification of this decision or direct administrative appeal to the Administrative Appeals Chamber of the National High Court. in accordance with Article 25 and paragraph 5 of the Fourth Additional Provision of Law 29/1998 of 13 July on Administrative Jurisdiction, within two months of the day following notification of this act, as provided for in Article 46 (1) of that Law.

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 interested party indicates their intention to lodge an administrative appeal. If this is the case, the interested party must formally inform the Spanish Data Protection Agency of this fact by submitting it via the Agency's electronic register [<https://sedeagpd.gob.es/sede-electronica-web/>] or through one of the other registers provided for in Article 16.4 of Law 39/2015 of 1 October. It shall also forward to the Agency the documentation proving that the administrative appeal has actually been lodged. If the Agency is not aware of the lodging of the administrative appeal within two months of the day following notification of this decision, it shall terminate the provisional suspension.

938-050522

Mar España Martí
Director of the Spanish Data Protection Agency