File identification

Resolution of sanctioning procedure no. no. PS 3/2023, referring to the Catalan Consumer Agency.

Background

1. On 10/27/2021, the Catalan Data Protection Authority received a letter in which a person filed a complaint against the Catalan Consumer Agency, an autonomous body attached to the Department of Business and Labor of the Generalitat, due to an alleged breach of the regulations on the protection of personal data.

Specifically, the complainant stated that the website of the Catalan Consumer Agency (hereafter, the Agency), and especially the form for presenting complaints *"was under an insecure connection"* . He stated that, for this reason, he had contacted the Agency's data protection representative, who would have replied that *"they will not do anything to solve it until January 2022"* . In order to substantiate his complaint, he provided two emails:

- An email that the complainant sent on 09/30/2021 to the Agency's *"LOPD Mailbox" address* (lopd.acc@gencat.cat) with the subject *"insecurity in forms with personal data"* , in which highlighted both what he considered to be an insecure connection from his corporate website - alluding to the lack of a secure certificate - as well as eventual *"problems with the leakage of personal data when filling out forms".* resulting from the lack of a secure certificate.

- A response email from the Agency, sent on 27/10/2021 from the address lopd.acc@gencat.cat to the person making the complaint, in which the following was noted:

  "(...) The consum.gencat.cat portal is currently being migrated, which will mean that the claim forms will also be under the https secure protocol . The forecast is that this migration will be completed next January. In any case, please note that the form data is sent to our case manager via a web service. This web service, which collects the data from the forms and sends them to the file manager, is indeed under a secure protocol (...)"

2. The Authority opened a preliminary information phase (no. IP 434/2021), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, on the common administrative procedure of public administrations (henceforth, LPAC), to determine whether the facts were susceptible to motivate the initiation of a sanctioning procedure.

3. In this information phase, on 04/11/2022 the Inspection Area of the Authority made a series of checks via the Internet on the facts subject to the complaint. Thus, it was found that the form on the Agency's website, for the formulation of claims or denunciations before this entity, had a website authentication certificate (with an encrypted connection). From the

result obtained, the corresponding due diligence was carried out.

4. On 11/11/2022, the Agency was required to report on various issues relating to the events reported.

5. On 12/20/2022, the Agency responded to the aforementioned request through a letter in which it set out the following:

- On whether on the date of the events reported (27/10/2021), the website of the Catalan Consumer Agency did not have an authentication certificate for its corporate website (SSL/TLS certificate or other), and no had the https protocol or other file transfer protocol implemented with encrypted connections; and if you currently have one:

  "On 27/10/2021 the main website (consum.gencat.cat) was not protected by an https certificate .
  Currently, a CDS consum.gencat.cat certificate is available (data below), migrating the entire system (website and forms that hang from it) on 11/17/2021.
  Below we reproduce the information from the production screenshot of the encrypted system as of November 2021. If necessary, we can send additional information in relation to the certificate as well as the exchange of emails with the application provider during the process validation of start-up.
  Data from the certificate generated in 2021, valid for 1 year. (...)

  Name: consum.gencat.cat
  (...)
  Application-
  Service-
  Department: EMT
  Type: SSL
  Authority: Sectigo

  The certificate was renewed last October of this year 2022. The Certificate is qualified under CA Sectigo (the certificate data shown below are the ones that can be seen and checked on the Agency's website).
  Current certificate data. (...)

- On whether during the period of time in which the Agency did not have an authentication certificate for its website, the sending and recording of personal data that was carried out through web forms (in any case , of the forms aimed at sending a claim), was carried out within the framework of a website authentication certificate (with an encrypted connection) and in its case, which certificate it was, and if it corresponded to a certificate qualified:

  " Although before November 2021, the GECO consum.gencat.cat website was not secure (HTTP), the calls to the destination system (SIC) to send the data from the web forms (including those for claims) are always have done by secure protocol (HTTPS). The invoked service is the following:
  https://empresa.extranet.gencat.cat/sicweb/AppJava/services/SicWebNvSOAP
  Below we provide the data of the service certificate invoked by the forms. There is evidence of the history of this certificate since 2015, currently renewed and with CA Sectigo until 2023 (capture below):

Name: empresa.extranet.gencat.cat
(...)
Application-
Service-
DepartmentEMC
TypeSSL
AuthorityCatCert

(...)"

- With regard to web forms, whether during the period of time when the Agency did not have a website authentication certificate, when a user submitted personal data (made a query, a claim, a complaint or a complaint, among others), after having sent the data, the response of the web service corresponding to the sending included personal data:

  "The response from the service invoked by the web forms does not contain personal data, it only contains a file number. As evidence of this point, we attach the following link through which you will be able to access the xml / descriptor file of the web service invoked by the forms: (...) ''

The Agency accompanied its letter with various documentation.

6. On 13/01/2023, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the Catalan Consumer Agency for an alleged infringement provided for in article 83.4.a), in relation to the Article 32.1, both of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereinafter, RGPD).

This initiation agreement was notified to said Agency on 01/13/2023.

In the initiation agreement, the Agency was granted a period of 10 working days to formulate allegations and propose the practice of evidence that it considered appropriate to defend its interests.

The deadline has been exceeded and no objections have been submitted.

proven facts

The main website of the Catalan Consumer Agency, consum.gencat.cat, for an indeterminate period of time, but in any case until 10/28/2021 as recognized by the entity, it did not have a certificate of 'authentication of your corporate website (SSL/TLS certificate or other), and did not implement the HTTPS protocol or any other file transfer protocol with encrypted connections , except for the sending and recording of data that was carried out through the web forms, which was carried out as part of a website authentication certificate (with an encrypted connection).

The Agency has certified that it has a CDS certificate issued on 28/10/2021 (renewed on 03/10/2022), and has stated that on 17/11/2021 it made effective the migration of its web pages to HTTPS.

Fundamentals of law

1. The provisions of the LPAC , and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of Catalan Data Protection Authority. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

2. In accordance with article 64.2.f) of the LPAC and in accordance with what is indicated in the agreement initiating this procedure, this resolution should be issued without a previous resolution proposal, given that the Agency has not made objections to the initiation agreement. This agreement contained a precise statement on the imputed liability.

3. In relation to the conduct described in the proven facts section, it is necessary to refer first to article 32.1 of the RGPD, relating to the security of the treatment, which determines the following:

> *"1. Taking into account the state of the art, the costs of application, and the nature, the scope, the context and the purposes of the treatment, as well as risks of probability and variable severity for the rights and freedoms of individuals, the person responsible and the person in charge of the treatment will apply appropriate technical and organizational measures*
> *to guarantee a level of security adequate to the risk, which in its case includes, among others:*
> *a) pseudonymization and encryption of personal data;*
> *b) the ability to guarantee confidentiality, integrity, availability and permanent resilience of treatment systems and services;*
> *c) the ability to restore the availability and access to personal data in a form fast in the event of a physical or technical incident;*
> *d) a process of regular verification, evaluation and assessment of the effectiveness of the technical and organizational measures to guarantee the safety of the treatment."*

In accordance with article 156.2 of Law 40/2015, of October 1, on the legal regime of the public sector, *"the National Security Scheme aims to establish the security policy in the use of electronic media in the scope of this Law, and is constituted by the basic principles and minimum requirements that adequately guarantee the security of the information processed"* .

The Royal Decree 3/2010, of January 8, which initially regulated, and in any case at the time of the alleged events, the National Security Scheme (ENS) in the field of electronic administration (from as provided for in article 42 of Law 11/2007, of June 22, already repealed), contained in its Annex II the security measures that needed to be implemented in order to achieve the fulfillment of the basic principles and minimum requirements established in the ENS. Among these security measures, section 5 contained the *protection measures (mp)* , and subsection 5.8.2, entitled " *Protection of web services and applications [mp.s.2]",* established the obligation to use website authentication certificates in all cases, that is to say, whether it was necessary to establish a low level in the measures of security, as a high level, as follows (emphasis ours):

"The subsystems dedicated to the publication of information must be protected against threats that are their own.
a) When the information has some type of access control, it must be guaranteed impossibility of accessing information bypassing authentication, in particular by taking measures
in the following aspects:
1st It must be avoided that the server offers access to documents through alternative routes to
certain protocol.
2nd URL manipulation attacks should be prevented.
3rd They must prevent manipulation attacks of fragments of information that are stored on the hard disk of the visitor of a web page through his browser, at the request of the server of the page, known in English terminology as " cookies ".
4th Code injection attacks must be prevented.
b) Privilege escalation attempts must be prevented.
c) Cross- site attacks must be prevented scripting ».
d) They must prevent manipulation attacks of programs or devices they carry out an action on behalf of others, known in English terminology as " proxies ", i special high-speed storage systems, known in English terminology as " caches ".

Low level

"Web site authentication certificates" will be used in accordance with European regulations (...).

High level

"Qualified Website Authentication Certificates" will be used .

During the processing of this procedure, the fact described in the proven facts section has been duly proven, based on the complaint and the attached emails submitted by the person making the complaint, but, especially, from the recognition in the previous phase by the Catalan Consumer Agency regarding the lack of implementation of an HTTPS protocol on the main website during the indicated time, which constitutes a breach of the obligation provided for in section 5.8.2 of the ENS then in force .

This would have made said website more vulnerable to computer attacks, such as *man -in-the - middle attacks* , in which the attacker acts as an intruder between the parties being communicating Thus, it could have been the case that a person entered data in a form on the Agency's website, in order to submit a claim, and that he had done so on a website that seemed identical to the one that this person was on visitor, but that in reality it was a fake website, which did not correspond to the official website of the Catalan Consumer Agency.

It is worth saying that the Royal Decree 311/2022, of May 3, which regulates the ENS currently in force, also provides in its section 5.8.2 that the systems that provide web services must be protected against the same threats contemplated in section 5.8.2 of the previous ENS.

This imputed fact, and now proven, constitutes an infringement, according to the provisions of article 83.4.a) of the RGPD, which typifies as such the violation of: "a) the obligations of the person in charge *and the person in charge of tenor of articles 8, 11, 25 to 39, 42 and 43; "*

The conduct addressed here has been included as a serious infringement in article 73.f) of Organic Law 3/2018, of December 5, on the protection of personal data and the guarantee of digital rights (hereinafter, LOPDGDD), in the following form:

> *" f) The lack of adoption of technical and organizational measures that are appropriate to guarantee a level of security adequate to the risk of the treatment, in the terms required by article 32.1 of Regulation (EU) 2016/679. "*

4. Article 77.2 LOPDGDD provides that, in the case of infractions committed by those in charge or in charge listed in art. 77.1 LOPDGDD, the competent data protection authority:

> *"(...) must issue a resolution that sanctions them with a warning. The resolution must also establish the measures to be adopted so that the conduct ceases or the effects of the offense committed are corrected.*
> *The resolution must be notified to the person in charge or in charge of the treatment, to the body to which it depends hierarchically, if applicable, and to those affected who have the status of interested party, if applicable."*

In terms similar to the LOPDGDD, article 21.2 of Law 32/2010 , determines that:

> *"2. In the case of violations committed in relation to publicly owned files, the director of the Catalan Data Protection Authority must issue a resolution declaring the violation and establishing the measures to be taken to correct its effects ."*

Given that in the previous phase the Agency certified, in relation to its main website, that it had a CDS certificate issued on 10/28/2021 (renewed on 10/03/2022), and stated that in date 11/17/2021 had effectively migrated its web pages to HTTPS, it is considered unnecessary to require the adoption of corrective measures.

For all this, I resolve:

1. Warn the Catalan Consumer Agency as responsible for an infringement provided for in article 83.4.a) in relation to article 32.1, both of the RGPD.

It is not necessary to require corrective measures to correct the effects of the infringement, in accordance with what has been set out in the 4th legal basis.

2. Notify this resolution to the Catalan Consumer Agency .

3. Communicate the resolution to the Ombudsman, in accordance with the provisions of article 77.5 of the LOPDGDD.

4. Order that this resolution be published on the Authority's website (apdcat.gencat.cat) , in accordance with article 17 of Law 32/2010, of October 1.

Against this resolution, which puts an end to the administrative process in accordance with articles 26.2 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, and 14.3 of Decree 48/2003 , of February 20, by which the Statute of the Catalan Data Protection Agency is approved, the imputed entity can file, with discretion, an appeal for reinstatement before the director of the Catalan Data Protection Authority Data, within one month from the day after its notification, in accordance with the provisions of article 123 et seq. of the LPAC. You can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

If the imputed entity expresses to the Authority its intention to file an administrative contentious appeal against the final administrative decision, the decision will be provisionally suspended in the terms provided for in article 90.3 of the LPAC.

Likewise, the imputed entity can file any other appeal it deems appropriate to defend its interests.

The director,