Litigation Chamber

Decision on the merits 141/2021 of 16 December 2021

File number: DOS-2020-03763

Subject: The exercise of the rights of the person concerned with regard to information systems

from a bank.

The Litigation Chamber of the Data Protection Authority, made up of Mr. Hielke Hijmans,

chairman, and Messrs. Dirk Van Der Kelen and Frank De Smet, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the prote

of natural persons with regard to the processing of personal data and to the free movement

of this data, and repealing Directive 95/46/EC (General Data Protection Regulation),

hereinafter “GDPR”;

Having regard to the Law of 3 December 2017 establishing the Data Protection Authority, hereinafter "LCA";

Having regard to the internal regulations as approved by the House of Representatives on December 20, 2018

and published in the Belgian Official Gazette on January 15, 2019;

Considering the documents in the file;

made the following decision regarding:

.

.

The defendant :

bank Y, represented by Me Erik Valgaeren and Me Carolien Michielsen, hereinafter "the

.

.

respondent"

.

.

I. Facts and procedure

A. Investigation by the Inspection Service

1. On April 22, 2020, the Management Board of the Data Protection Authority (hereinafter the DPA)
decided to refer the matter to the APD Inspection Service on the basis of Article 63, 1° of the LCA.
Following Decision No. 01/2019 taken by the Litigation Chamber on May 15, 2019 and the subsequent judgment
of the Court of Markets of October 9, 2019, the Management Committee noted that there was
serious indications of practices that may give rise to violations of the fundamental principles
of the protection of personal data. The Management Committee therefore seized the
Records Inspection Service by requesting an investigation into the extent to which
the defendant's information systems enable the exercise of human rights
concerned, in particular the right to rectification (Article 16 of the GDPR). This means that the Service
of Inspection is seized in order to check if the information systems of the defendant are in conformity
the requirements set by the GDPR in terms of exercising the rights available to any person
concerned1 in its capacity as a customer of the defendant.
2. The Inspection Department sent its report of March 23, 2021 to the Litigation Chamber on the
basis of Article 91, § 2 of the LCA, involving referral to the Litigation Chamber under
Article 92, 3° of the LCA.

B. Proceedings before the Litigation Chamber

3. On April 6, 2021, the Litigation Division decides, pursuant to Article 95, § 1, 1° and Article 98 of
the ACL, that the case can be dealt with on the merits.
4. On the same day, the defendant is informed by registered mail of this decision and of the
inspection report and inventory of the documents in the file which was sent to the Chamber
Litigation by the Inspection Service. Likewise, the defendant is informed of the provisions of
Article 98 of the LCA and, pursuant to Article 99 of the LCA, he is informed of the deadlines for introducing
its findings. The deadline for receipt of the respondent's submissions in response was

set for May 28, 2021.

5. On May 10, 2021, the defendant requests a copy of the file (art. 95, § 2, 3° of the LCA), which is

transmitted May 12, 2021. Respondent also agrees to receive all communications

1 Decision No. 01/2019 of 15 May 2019, on the other hand, only concerns the safeguarding of the rights of a single specific plain

the personal data were processed by the defendant, given that the Litigation Chamber had only been seized

for this treatment in the complaint.

relating to the case electronically and expresses its intention to make use of the possibility of being

of course, this in accordance with Article 98 of the LCA.

6. On May 28, 2021, the Litigation Chamber receives the defendant's submissions in response in

which it is requested, in main order, to find that there is no violation of articles 5.1

c), d) and f), 5.2, 12, 16, 24, 25, 30.1, 31, 32, 38.3 and 38.6 of the GDPR and, in the alternative, to keep

mitigating circumstances into account when imposing a sanction.

7. On July 14, 2021, the parties are informed that the hearing will take place on September 30, 2021.

8. On September 30, 2021, the defendant is heard by the Litigation Chamber and thus has the opportunity

to put forward his arguments. The Litigation Division decides to continue the case in order to

to allow the defendant, after the expiry of the deadline of November 15, 2021 which he himself has advanced,

namely the date on which the introduction of diacritics in surnames and first names in

its applications should be carried out, to come and explain the new computer system.

A new hearing will be scheduled for this purpose shortly after this date.

9. On October 1, 2021, the Respondent is informed that the hearing to bring the case to trial

continuation will take place on November 22, 2021.

10. On October 12, 2021, the minutes of the hearing of September 30, 2021 are sent to the defendant,

in accordance with Article 54 of the DPA's internal rules. The defendant thus has the opportunity

to have any comments added to the minutes as an appendix.

11. On October 19, 2021, the Litigation Chamber receives some remarks from the defendant regarding the

minutes, which it decides to resume in its deliberation once the meeting scheduled for

November 22, 2021 will have taken place.

12. On November 22, 2021, the defendant was heard by the Litigation Chamber and he explained the

realization of the introduction of diacritics in the surnames and first names in its

apps.

13. On November 23, 2021, the minutes of the hearing of November 22, 2021 are submitted to the Respondent,

in accordance with Article 54 of the DPA's Internal Rules. The defendant sees himself as

offer the opportunity to add any comments in this regard to the appendix to the

minutes, without this implying a reopening of the debates.

14. On November 23, 2021, the Litigation Chamber notified the Respondent of its intention to

proceed with the imposition of an administrative fine as well as the amount thereof, in order to give

the defendant the opportunity to defend himself before the penalty is actually imposed.

15. On November 29, 2021, the Litigation Chamber receives the comments with regard to the minutes of

the hearing which took place on November 22, 2021, remarks that the Litigation Chamber resumes in

his deliberation.

16. On December 14, 2021, the Litigation Chamber received the defendant's reaction concerning

the intention to impose an administrative fine, as well as the amount thereof. The defendant

argues that a number of mitigating circumstances which have been set out in the

conclusions for Y Belgium and during the hearing, were not taken into consideration by the

Litigation Chamber given that they do not appear in the sanction form and that

the proposed fine is disproportionately high compared to the decision on the merits

n° 18/2020 of April 28, 2020 for an identical violation.

II. Motivation

17. The Litigation Chamber assesses below each of the findings set out in the report of the

Inspection Service in the light of the pleas put forward in this respect by the defendant.

a) Principle of accuracy (Article 5.1 d) GDPR), accountability (Article 5.2 GDPR), information□

transparency, communication and other modalities for the exercise of human rights□

data subject (Article 12 of the GDPR), the right to rectification (Article 16 of the GDPR), the protection of□

data by design and data protection by default (article 25 of the GDPR) and□

obligation to cooperate (Article 31 of the GDPR)□

18. The first item under investigation by the Inspection Service concerns the assessment of□

the extent to which the respondent has made the necessary modifications in order to implement□

diacritics in its ICT systems.□

19. The Inspection Service finds that the defendant cannot create a technical image of the system□

in terms of planning for the implementation of diacritics in the current ICT system□

(applications + mainframe) and any initial results showing the efforts made.□

Furthermore, the Inspection Service also finds that the defendant remains in the "phase□

exploratory" of preliminary study and discussion, without wanting to achieve objectives and□

concrete results.□

20. The Inspection Service comes to the conclusion that the defendant is in violation of articles□

5.1 d, 5.2, 12, 16, 25 and 31 of the GDPR because he is unwilling or unable to submit a concrete planning with□

concrete results and is also unwilling or unable to demonstrate technical changes□

of the system having a positive impact on the initial request of the data subject. According to□

Inspection Service, the situation since the decision taken by the Litigation Chamber on May 15□

2019 (with the exception of carrying out preliminary study work (feasibility)) remained unchanged□

and therefore did not improve.□

21. The Inspection Service makes the following points in this respect:□

o The defendant has IT applications and database systems (around 150) of which□

the central client system which is a mainframe system which was commissioned in 1995.□

This central client system only supports EBCDIC ("extended binary-coded decimal□

interchange code"). Although diacritics have meanwhile been added to the

EBCDIC table, the defendant made no changes in the client system

central. In 2020, the defendant is still using a computer system that dates from 1995 and

which does not allow the exercise of the right of rectification.

o Regarding the number of underlying applications that interact with the

central customer system, which require modification following the introduction of the signs

diacritics, the Inspection Service finds that the defendant mentions 150 applications

in his initial letter of November 6, 2019 and it was not until November 2, 2020 that he was

able to provide a list corresponding to the precise number as mentioned on

November 6, 2019, supplemented by the correct technical name of the system and the

duplicate filtering. The Inspection Service points out in this respect that the defendant

often answered that the analysis was not yet closed, which is strange given

the number of months elapsed, the number of staff members, the financial and

the possibilities of the defendant.

o With respect to very old large systems about which the defendant asserts

November 6, 2019 that their adaptation will last 18 months, the Inspection Service notes

that the defendant does not provide until November 2, 2020 a list describing these systems and the

specifically quoting.

o Investigating change management and the plan of approach to proceed with

the implementation of the technical proposals, the Inspection Service tries to make a

idea of process development and how implementations are

carried out within the defendant. The Inspection Service finds that the defendant indicates

September 16, 2020 that the changes to be made for the introduction

letters with accents will be done according to the AGILE principle in force within Y, which

implies that the defendant will solve the limitation of letters with accents in small steps

synoptics.

On October 12, 2020, the defendant indicated that it had taken initiatives to resume the

diacritics in the central client system; a 4-phase approach is followed and at

At this time, phases 1 and 2 are processed:

1) analysis of all potentially affected systems and applications;

2) adaptations of these systems in the test environment and testing of these

individual manner with regard to the processing of diacritics;

3) creation of test chains in order to guarantee the consistency of the applications;

4) concrete realization of the modifications.

Decision on the merits 1412021 - 6/26

On November 2, 2020, the defendant documents how AGILE was translated within

of its organization and provides information on the feasibility study in the form of

two diagrams concerning the testing approach.

The Inspection Service comes to the conclusion that it is strange to have only a few

structured and generic information to follow this adaptation in a global way.

With the exception of general information about the AGILE approach and the study phase

preliminary, the defendant cannot provide information demonstrating a possible

progress or concrete results that can have a positive impact on the person

concerned and the exercise of their rights.

o Following the review of the technical design, the inspection report contains the diagrams

techniques concerning architectural design where the defendant indicates each time if, and the

if applicable to what extent, modifications may have an impact on each

of the parties, both for the central client system, the supporting technologies and

underlying – middleware, mainframe Z applications, non-mainframe Z applications,

non-mainframe applications – only for front-end channels and applications.

Articles 5.1. d), 12 and 16 GDPR

22. The defendant argues that Articles 5.1 d), 12 and 16 of the GDPR are respected, which he argues

as following :

- The exercise of the rights of the data subject is facilitated in accordance with Article 12 of the GDPR

the fact that customers can adapt their data themselves via the applications to

Internet banking transactions or have them adapted by front office staff.

The privacy statement also mentions the useful contact details for exercising the right

of rectification. In addition, there is also an internal thread and documentation of

procedures for exercising the rights of data subjects. The necessary processes have

have also been implemented in order to adequately process requests to exercise rights.

- The right of rectification (article 16 of the GDPR) is respected for all requests for adaptation

or rectification. The impossibility faced by the defendant to follow up on the request

adaptation is limited to the treatment of diacritics in a name.

- - The realization of a complex IT project with adaptations of many systems, which requires

a lot of time and investment to respond to an absolute minority of requests for

rectification, should not be considered, according to the defendant, as a reasonable measure in the

meaning of Article 5.1 d) of the GDPR.

- The defendant indicates that the judgment of the Markets Court of October 9, 2019 is still pending

before the Court of Cassation and that while awaiting the pronouncement, one cannot simply affirm

Decision on the merits 1412021 - 7/26

that articles 5.1 d), 12 and 16 of the GDPR are not respected due to the lack of indication of

diacritics.

23. Defendant's submissions indicate that it was originally intended to implement the signs

diacritics in its ICT systems as part of the "UNITE" ICT project already underway in 2019 in

within Group Y, which aimed to fully harmonize the systems and applications of the entities

Y in Belgium with those of Y entities in the Netherlands; however, the UNITE project turned out to be too

ambitious and in 2020 the defendant had to carry out alone, therefore without Y Netherlands, the adaptations

useful system techniques. On the basis of this statement, the Litigation Chamber finds

that the intention to use the diacritics in the defendant's applications existed, but

that this did not materialize due to the dissociation of the defendant within the UNITE project.

The Respondent now asserts in the pleadings that the incorporation of the diacritical marks in

applications presupposes going beyond reasonable limits, while Article 5.1 d) of the

GDPR only requires the respondent to take all reasonable steps to ensure that the

personal data which are inaccurate, having regard to the purposes for which they are

processed, erased or rectified without delay.

24. Based on the inspection report, the Litigation Chamber finds that the client system

central, which is the heart of the bank because customer data is stored there

centrally and extracted from it by related systems, is a mainframe system that has

was put into service in 1995. Although the diacritics have meanwhile been added to the

EBCDIC table, the defendant did not make changes in the central client system that

supports EBCDIC. This means that the defendant did not exploit this possibility to adapt its

system.

25. Although the reasonableness of taking this measure is disputed by the Respondent,

the Litigation Chamber considers that it is normal that the customer whose data

personal are treated within the framework of its financial relationship with the bank expects that

his name is indicated correctly, precisely in view of the importance of the accuracy of

data when providing financial services and products. The Litigation Chamber refers

also in this respect to the judgment of the Court of Markets of October 9, 2019 which specifies that one can

expect a well-functioning banking institution to have a program

computer that meets current standards, including the aforementioned right to correct spelling

by name. And the Court added that the right of rectification is a fundamental right2. It is therefore

2 The decision of the Market Court is worded in the following terms:

“[…]

The fact that it would technically require "effort" to use a computer program that puts the accents on the letters

uppercase doesn't matter and is irrelevant.

"Stating now (in 2019!) that adapting a computer program would require several months and/or an additional financial cost

for the banking institution, does not allow SA Y BELGIQUE to ignore the rights of the data subject. The rights that are

attributed to the person are similar to performance commitments on the part of the party processing the personal data

personal.

reasonable for the bank to take the measures available to it to process the names of

customers with diacritics and thus to adapt the system to the current possibilities

mainframe which has been in service since 1995. With respect to the defendant's argument that

such adaptation not only of its central client system but also of the sub-systems

underlying or related assets requires a lot of time and investment, which cannot be

considered reasonable, the Litigation Chamber notes that this is generally

specific to any fundamental change in computer systems, which is all the more

when it comes to old systems as in the present case. The need to devote time and

investments for appropriate computer systems in order to be able to process signs

diacritics is not limited (contrary to what the defendant claims) to an absolute minority

requests for rectification but is necessary in the interest of any client whose name contains

diacritics. The starting point must indeed be that the defendant, like

any data controller, make every effort to process accurate data

and does not adopt a passive attitude and therefore does not wait for a request from a client to make

change its name to undertake an action to achieve this adaptation.

26. The Litigation Chamber therefore considers that the impossibility of the defendant to proceed until

present at the rectification of the name of clients who request the indication of diacritics in

their name violates GDPR Article 5.1(d). It is also a violation

of Article 16 of the GDPR, since the defendant is not in a position to fully comply

the right of rectification. The Respondent asserts that all requests for accommodation or

rectification are carried out, except for the request for adaptation of diacritics. This brings the
Litigation Chamber to conclude that the defendant does not follow up on any exercise of the right of
correction. The right of rectification must however be respected in all its facets.

27. When determining the penalty for these violations, the Litigation Chamber nevertheless takes
account of the declaration of the defendant to undertake to have carried out, by November 15, 2021,
all the adaptations necessary to be able to integrate the diacritics in the names and
first names in its applications. As part of this performance commitment, the defendant
formulates two warnings of which the Litigation Chamber takes note:

1° In accordance with the industry standard in force worldwide, diacritics are not
are not included on bank cards. If the defendant did so, it could cause problems when
the use of the bank card, both online and offline. Regarding payments
(SEPA), all Belgian banks have also agreed to limit themselves to all
of standard marks, without diacritics.

A well-functioning bank can be expected that – when it uses a computer program – it uses a
that meets current standards, including the aforementioned right to the correct spelling of the name. The right of rectification is a
fundamental.

[…]"

Decision on the merits 1412021 - 9/26

2° The indication of diacritics on the printed extracts of credit cards will only be available
only at a later date.

During the hearing on November 22, 2021, the defendant gives a presentation which testifies
enough of the fact that the necessary steps have been taken to treat the signs
diacritics in the names of clients, so that the Litigation Chamber can observe a
progress on this point. With specific regard to the Complainant in Decision No. 01/2019
of May 15, 2019, the defendant also demonstrates that the diacritical mark in his name is treated.

28. With regard to Article 12 of the GDPR, the Litigation Chamber finds that the defendant

sufficiently demonstrates that there is transparent communication with clients in order to

inform them of the exercise of their rights, and that the necessary means are made available to

exercise these rights, the defendant thus facilitating the exercise of these rights. Moreover, it does not appear from

inspection report that the defendant would not conduct transparent communication (article

12.1 GDPR). The inspection report only indicates that for the defendant, it is not

possible at the technical level of the system to respond to a request for rectification

regarding diacritics, but that does not preclude the defendant from actually facilitating

the exercise of the rights of its customers (article 12.2 of the GDPR) via the banking applications by

Internet or with the help of front office staff, even if the defendant is not able

to take appropriate action and immediately proceed with the rectification insofar as

the request relates to diacritics (Article 16 of the GDPR). It follows that we cannot

finding a violation of Article 12 of the GDPR.

29. With regard to the Respondent's assertion that the Litigation Division could not

not proceed to the observation of a violation of articles 5.1 d), 12 and 16 of the GDPR for cause

absence of indication of diacritics, due to the proceedings pending before the Court of

cassation lodged by the defendant against the judgment of the Court of Markets rendered following the

Decision No. 01/20193 of the Litigation Chamber, the Litigation Chamber points out that the

appeal in cassation constitutes an extraordinary appeal which does not have a suspensive effect. That means

that pending the judgment of the Court of Cassation, the judgment of the Court of Markets produces

its effects fully and that the Inspection Service could seize the Litigation Chamber via the

inspection report of March 23, 2021 and that therefore, the Litigation Chamber can take

this decision on the merits.

GDPR Article 25

30. The Respondent asserts that the Inspection Service finds an alleged violation of Article 25 of the

GDPR but does not explain what this violation consists of.

3 Decision No. 01/2019 of 15 May 2019 relating to a complaint for non-compliance with the request for correction of the spelling

31. The Litigation Chamber considers that the inspection report clearly demonstrates that for its central client system, the defendant is still using a mainframe which has been put into service in 1995 and notwithstanding the technical possibility of integrating and processing the signs diacritics, he chose not to harmonize his system in this sense. According to article 25 of the GDPR, the state of the art which allows the processing of diacritics requires that the respondent takes the appropriate technical and organizational measures in order to carry out effectively the principles of data protection, including the principle of accuracy, and to integrate the guarantees necessary in the processing to comply with the requirements of the GDPR and to protect the rights of data subjects.

32. The Respondent indicates that Article 25 of the GDPR also cites, as a criterion for determining the appropriate measures, the costs of implementation as well as the risks associated with the processing, including the degree of probability and seriousness varies, for the rights and freedoms of natural persons. The defendant claims in this respect that there is no risk as regards the identification of the person as to the concrete use of a certain name without indication of the specific diacritical mark. In addition, the realization of a very complex IT project with adaptations of many systems requires a lot of time and investment in order to be able to respond to an absolute minority requests for rectification and therefore, according to the defendant, the risk is extremely limited in terms of seriousness and likelihood for the rights and freedoms of natural persons.

33. The defendant's assertion that there is no risk of identification of the person concerned in the absence of processing of the diacritics and that the risk is extremely limited given the low number of requests for rectification concerning diacritical marks cannot not imply, according to the Litigation Chamber, that the defendant remains totally in default, as in this case, to take the slightest measure to be able to respond to any rectification requests.

34. Furthermore, the Respondent refers to Guidelines 4/2019 relating to Article 25 - Protection

data by design and data protection by default4 which provide at the level of

the accuracy of the data that the requirements laid down by Article 5.1 d) of the GDPR must be

considered according to the risks and consequences of the concrete use of the data.

The defendant considers that it can be inferred from this that the measure consisting in the integration of the signs

diacritics in its systems is not proportionate to the risks for the data subject.

The defendant forgets, however, the fact that, with regard to the protection of data from the

design and data protection defaults in terms of accuracy, the guidelines

relating thereto specifically provide with regard to erasure/rectification that the

controller deletes or rectifies inaccurate data without delay. Guiding lines

thus confirm what Article 5.1 d) of the GDPR provides, namely that any data controller

4 https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fr.pdf

has the obligation to delete or rectify inaccurate data without delay and that it is not the responsibility of the

responsible for processing whether or not to grant a request for the erasure or rectification of

inaccurate data due to financial considerations or risk analysis.

35. The fact that the defendant did not adapt its IT systems to allow the processing of signs

diacritics in the name of the customers if a request is made to this effect, there is a violation of

GDPR Article 25. The Respondent argues that in the meantime, namely since Decision 01/2019

of May 15, 2019 and the inspection report in question, it has already made numerous efforts to

make its systems compliant with the GDPR with regard to the processing of diacritics, which

which is also an important element in determining the penalty for this violation.

However, this cannot give rise to a retroactive cancellation of the violation.

36. Considering the efforts made in the meantime by the defendant as well as the seriousness and the limited risks for

the fundamental rights of the persons in question, in the light of recital 75 of the GDPR, the

Litigation Chamber decides, despite finding violations of Articles 5.1.d), 16 and 25

of the GDPR, not to proceed with the imposition of a sanction for these violations. She then orders

a dismissal, under article 100, § 1, 2° of the LCA.

GDPR Articles 5.2 and 31

37. In the report of the Inspection Service, it appears on several occasions that it was necessary to address several

letters to the defendant asking him to provide concrete answers to the questions asked, in

as a result of which the Inspection Service deduces that the defendant has not complied with his

responsibility and its obligation to cooperate. The Inspection Service is also surprised that there

has little structured and generic information to track adaptations globally.

With the exception of general information about the AGILE approach and the study phase

preliminary, the Inspection Service considers that the defendant cannot provide information

demonstrating a possible breakthrough or concrete results that can have a positive impact on

the data subject and the exercise of his rights and freedoms.

38. On the basis of the documents provided by the defendant, the Litigation Chamber must however find

that through the required documentation, the defendant can demonstrate the extent to which the

GDPR is respected. Not only has the defendant made available a common thread and a

internal documentation of procedures for exercising the rights of data subjects, but

it also specifically made available documentation relating to the IT project dedicated to

the implementation of diacritics as well as the processes that demonstrate the progress of the

project. Thus, the Respondent has documented which steps have already been undertaken as well as those it

will undertake again in the future. To explain the time needed to answer the questions

raised by the Inspection Service during the various phases, the defendant declares that a

in-depth analysis was required to determine which applications may be impacted

by adding diacritics and that this was not immediately possible. The defendant

asserts that it took time to carry out analyzes and tests in order to then carry out the

adaptations in a controlled manner, without jeopardizing the stability of its systems. In this regard, the

Litigation Chamber finds on the basis of the documents that the defendant has provided sufficient

documentation demonstrating incontestably the progress in the file and the results

concrete, so that no violation of Article 5.2 GDPR can be established.

39. The Litigation Division also assessed the findings of the Inspection Service at the

light of the defendant's obligation to cooperate and finds that the Inspection Service did not

sufficiently demonstrated that the defendant had not attempted through response letters from

respond in detail and in detail to the questions asked. Furthermore, the defendant

declared on several occasions willing to engage in consultation, in addition to this

approach. It cannot therefore be established that he disregarded the obligation to cooperate with

the supervisory authority.

40. The Litigation Chamber therefore considers that no violation of Article 31 of the GDPR can be

observed. This judgment is based on findings of fact, making a judgment of

principle in this case regarding the scope of the duty to cooperate.

b) Principle of data minimization (article 5.1 c) of the GDPR), integrity and confidentiality

(Article 5.1 f) GDPR), liability (Article 5.2 GDPR), liability of the controller

processing (Article 24 of the GDPR), data protection by design and protection

default data (Article 25 of the GDPR) and security of processing (Article 32 of the GDPR)

41. The Inspection Service finds that the respondent uses the surname of the complainant5 in:

- internal notes for the "Data Council" and presentations of the latter

-

exchange of e-mails and ICT tests

concerning the ICT program on the use of diacritics.

42. The Inspection Service concludes that this processing activity of the defendant constitutes a

violation of Articles 5.1 c) and f), 5.2, 24, 25 and 32 of the GDPR, conclusion which is based on the

consideration that the use of the complainant's surname is not necessary for the purpose

for which it is treated and can therefore be avoided. The name of the project or business could have a

Complainant's alternate name and surname has no added value. According to the Inspection Service,

there are various words in other languages with diacritics that can be used for this

Indeed, the use of the complainant's surname can be stigmatizing and because of its dissemination

within its organization, the Respondent has no control in this regard. The inspection report

5 The Inspection Service refers to the complainant in Decision No. 01/2019 of 15 May 2019

Decision on the merits 1412021 - 13/26

concludes that using the surname as a "test person" or as a "case" is not

not proportionate:

-

the application of the basic principles of "data minimization" and "integrity and

privacy" ;

-

-

the appropriate technical or organizational measures to be taken;

the guarantee of confidentiality, integrity, availability and resilience of its systems of

treatment and its services;

-

to the obligation of contractual discretion (banking) or to the discreet processing of data to

personal character as a bank vis-à-vis the customer.

43. The Litigation Chamber asserts that the surname of the complainant in Decision No. 01/2019

of May 15, 2019 does indeed constitute personal data within the meaning of Article 4.1) of the

GDPR, given that the complainant is identifiable by means of Decision No. 01/2019 issued by the

Litigation Chamber and the judgment of the Markets Court of October 9, 2019, in which the

defendant was on each occasion a party and that the identity of the plaintiff was therefore known to him. It results

that the Complainant can be directly identified by only his last name within

defendant's organization, since they were both parties to the litigation. According to

Litigation Chamber, the use of the surname as a project name must be

considered as processing based on the legitimate interest of the defendant (article 6.1 f) of the GDPR).

44. In accordance with Article 6.1.f) of the GDPR and the case law of the Court of Justice of the European Union

European Union (hereinafter "the Court"), three cumulative conditions must be met for a

controller, i.e. the defendant, can validly invoke this ground

of lawfulness, "namely, first, the pursuit of a legitimate interest by the controller of the

treatment or by the third party or third parties to whom the data is communicated, secondly, the

necessity of the processing of personal data for the fulfillment of the legitimate interest

pursued and, thirdly, the condition that the fundamental rights and freedoms of the person

concerned by data protection do not prevail" (judgment "Rigas"6).

45. In other words, in order to be able to invoke the basis of lawfulness of "legitimate interest"

in accordance with Article 6.1.f) of the GDPR, the controller must demonstrate that:

- the interests it pursues with the processing can be recognized as legitimate (the "test of

purpose");

- the envisaged processing is necessary to achieve these interests (the “necessity test”); and

6 CJEU, 4 May 2017, C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA „Rī

satiksme”, recital 28. See also CJEU, 11 December 2019, C-708/18, TK c/ Asociația de Proprietari bloc M5A-ScaraA,

recital 40.

- the weighting of these interests in relation to the interests, freedoms and fundamental rights of

data subjects weighs in favor of the controller (the "weighting test").

46. With regard to the first condition (the "purpose test"), the Litigation Chamber considers that

the purpose of executing both the aforementioned decision of the Litigation Chamber and the judgment

of the Court of Markets7 can be qualified as being prosecuted for a legitimate interest.

According to recital 47 of the GDPR, the interest that the defendant pursued as

controller can in itself be considered legitimate. The first requirement

included in Article 6.1.f) of the GDPR is therefore fulfilled.

47. In order to fulfill the second condition, it must be demonstrated that the processing is necessary for the achievement of the aims pursued. More specifically, this means asking whether the same result cannot be achieved with other means, without data processing to personal nature or without unnecessary substantial processing for the data subject.

48. Given that the Respondent was each time a party to the proceedings before the Chamber Litigation and the Court of Markets, the identity of the complainant was already known within a circle limited number of people from the defendant's organization.

49. Further, the Respondent states that the surname was used in documents purely internal and confidential within the Data Council composed of only 7 members as well as in a few emails limited to the strictly necessary people involved in the project. He ... not There is no evidence that the processing of the complainant's surname was unnecessarily invasive for the person concerned. The Litigation Chamber thus considers that the defendant did not not processed the surname of the data subject in disregard of the principle of minimization of data, so the second condition is met.

50. In order to check whether the third condition of Article 6.1.f) of the GDPR - the so-called "test of balancing" between the interests of the controller on the one hand and the freedoms and rights fundamentals of the data subject on the other hand - can be fulfilled, in accordance with the recital 47 of the GDPR, the reasonable expectations of the person must first be taken into account concerned. In particular, it must be assessed whether "the data subject can reasonably expect, at the time and in the context of the collection of personal data, that they are processed for a given purpose"8.

7 See in the same sense decision on the merits 35/2020 of 30 June 2020, point 28.

8 Recital 47 GDPR.

51. This aspect is also underlined by the Court in its judgment "TK v. Asociația de Proprietari bloc M5A-ScaraA" of December 11, 20199, which states the following:

"Also relevant for the purposes of this balancing are the reasonable expectations of the
data subject that his or her personal data will not be processed when,
in the circumstances of the case, that person cannot reasonably expect a
further processing thereof.

52. It follows both from decision no. 01/2019 taken by the Litigation Chamber on 15 May 2019 and from
the decision of the Markets Court of October 9, 2019 that the defendant had to adapt its applications,
at least with regard to the treatment of diacritics in the surname of the
concerned person. That
necessarily implies that
the person concerned could
reasonably expect10 that his surname will be used within the organization of the
respondent in order to meet the requirements set out in the aforementioned decision of the Chamber
Litigation and in that of the Court of Markets.

53. All of the aforementioned elements lead the Litigation Chamber to conclude that the defendant
processed the surname of the data subject legitimately within its organization
pursuant to Article 6.1 f) of the GDPR and that no element is advanced to affirm that the defendant
would have acted contrary to the requirements of the GDPR, so that on the part of the defendant, no
violation of Articles 5.1 c) and f), 5.2, 24, 25 and 32 of the GDPR has been committed.

c) Position of the Data Protection Officer (Article 38.3 and 38.6 GDPR)

54. With regard to the position of the data protection officer, the report of the Service
of Inspection finds that there is a conflict of interest on his part and that he does not report
directly to the highest level of the management body.

55. With regard to the requirement of direct reporting to the highest level of management (Article 38.3
of the GDPR), it is underlined in the defense that the Data Protection Officer reports to

9 CJEU, 11 December 2019, C-708/18,TK v/ Asociația de Proprietari block M5A-ScaraA, recital 58.

10 Recital 47 GDPR. The legitimate interests of a controller, including those of a controller to

whom the personal data may be communicated, or of a third party may constitute a legal basis for the
processing, unless the interests or fundamental rights and freedoms of the data subject prevail, taking into account the
reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest
could, for example, exist where there is a relevant and appropriate relationship between the data subject and the data controller
processing in situations such as where the data subject is a customer of the controller or is at his
service. In any event, the existence of a legitimate interest should be carefully assessed, in particular in order to
determine whether a data subject can reasonably expect, at the time and in the context of data collection, to
personal character, that they are processed for a given purpose. The interests and fundamental rights of the
data subject could, in particular, prevail over the interest of the controller when personal data
personal are processed in circumstances where the data subjects do not reasonably expect processing
ulterior. Since it is up to the legislator to provide by law the legal basis for the processing of personal data
personal data by public authorities, this legal basis should not apply to processing carried out by public authorities.
public in the performance of their duties. The processing of personal data strictly necessary for
purposes of fraud prevention also constitutes a legitimate interest of the data controller concerned. The treatment of
personal data for the purposes of commercial prospecting can be considered as being carried out to respond to a
legitimate interest. [proper underlining].
Decision on the merits 1412021 - 16/26
the Executive Committee, also called the Management Committee, via the Chief Risk Officer (CRO) who
itself sits on the Executive Committee, which is the highest body. The defendant points out
that the reporting line goes directly from the Data Protection Officer to the Executive
Committee. The report to a body can only be made via a natural person, namely by
the species the CRO which serves as an access point to this body. The defendant justifies this choice of the CRO because
that he is a member of the Executive Committee, which is the main contact for the Risk Committee
who takes cognizance of all important privacy issues.
56. The Data Protection Officer is himself a permanent member of the Data Council, which is
a delegated sub-committee and an extension of the Executive Committee, the decisions of the Data

Council being binding on the Executive Committee. The defendant points out that the presence
of the data protection officer in the Data Council constitutes a form of report to the
highest level.

57. Respondent also adds that the Executive Committee is a collegial body, the CEO having
a single voice in the decision-making process, just like all the other members of this body.
The Respondent points out during the hearing that the DPO should not report to the most senior individual,
namely the CEO, within the highest body, but that the report at the highest level is sufficient.
In addition, all other members of the Executive Committee, including the CEO, are responsible
of departments that process data. It follows, according to the defendant, that one cannot
claim that a certain member of the Executive Committee would be more neutral than the others
members.

58. On the basis of the documents supporting the explanation given by the defendant, the Litigation Chamber
considers that no violation of Article 38.3 of the GDPR can be established.

59. With regard to the finding of the Inspection Service that there is a conflict of interest in the
head of the data protection officer (article 38.6 of the GDPR) due to the fact that he is also the head
Operational Risk Management (ORM), Information Risk Management (IRM) and Special
Investigation Unit (SIU), the defendant argues that the head of these services has no jurisdiction to
decision on the purposes and means of the operational processing of data to
personal character, but only a competence of opinion and control.

60. During the hearing, the Litigation Chamber examined the impact that the delegate for the protection of
data has on the decision-making process because of its other functions.

61. The Litigation Chamber notes that the Respondent insists in its submissions on the
purely advisory and control skills of each of the three departments, namely Operational Risk
Management, Information Risk Management and Special Investigation Unit. The defendant considers
thus being able to affirm that the data protection officer has no tasks (also via his
functions in each of the departments in question) under which he could take

decisions as to the purpose and means of any processing of personal data

personal.

62. The Litigation Chamber considers that it has not been demonstrated that the delegate for the protection of

data, who is also head of department of each of these departments and therefore endorses a

position of responsibility, does not carry out any task that is incompatible with his position as

data protection officer.

63. The Litigation Division points out in this context that the role of advising and controlling

departments as such does not mean that they do not define the purpose and means of

data processing.

64. The Litigation Division must assess how and to what extent the independence of

of the data protection officer with regard to each of these three departments (of which he is

head of Service).

65. The defendant therefore himself designates the same natural person as responsible for

each of the three departments and as delegate to

data protection.

This responsibility for each of these three departments unquestionably implies that this

person, in this capacity, determines the purposes and means of the data processing to

personal character within these three departments and therefore is responsible for the processes of

processing of data relating to Operational Risk Management, Information Risk

Management and Special Investigation Unit, as noted in the inspection report.

66. Group Guidelines 29 on Data Protection Officers 11

explain that the data protection officer cannot exercise within the organization a

function which leads it to determine the purposes and means of the processing of personal data

11 Article 38(6) allows DPOs to "carry out other assignments and tasks". However, it requires the organization to ensure that

"these missions and tasks do not entail any conflict of interest".

The absence of conflict of interest is closely linked to the obligation to act independently. Although DPOs are allowed to exercise other functions, a DPO may only be entrusted with other missions and tasks if these do not give rise to a conflict interest. This means in particular that the DPO may not exercise a function within the organization which leads him to determine and means of processing personal data. Due to the specific organizational structure of each organization, this aspect must be studied on a case-by-case basis.

As a general rule, functions that may give rise to a conflict of interest within the organization may include functions senior management (e.g. general manager, operational manager, financial manager, chief medical officer, head of marketing department, human resources manager or IT department manager), but also other roles at a lower level of the organizational structure if these functions or roles imply the determination of the ends and the means of the treatment. In addition, there may also be a conflict of interest, for example, if an external data protection officer is called to represent the controller or the processor before the courts in cases relating to questions relating to the Data protection.

Depending on the activities, size and structure of the organization, it may be good practice for data controllers or the subcontractors: • to identify the functions that would be incompatible with those of DPD; • establish internal rules to this ef in order to avoid conflicts of interest; • include a more general explanation regarding conflicts of interest; • to declare that their DI has no conflict of interest with respect to his function as DPO, with the aim of raising awareness of this requirement; • to provide guarantees in the internal regulations of the organization and to ensure that the vacancy notice for the function of DPO or the se be sufficiently precise and detailed to avoid any conflict of interest. In this context, it should also be borne in mind that the Conflicts of interest can take different forms depending on whether the DPO is recruited internally or externally.

WP243Rev01, paragraph 3.5, emphasis by the Litigation Chamber. These guidelines have been endorsed by the Committee European Data Protection Authority (EDPB).

personal. It is therefore a substantial conflict of interest. The role of service manager is not therefore not reconcilable with the function of data protection officer who must be able to carry out its tasks independently. The accumulation, on the part of the same natural person, of the function of head of each of the three services in question separately on the one hand and

of the function of data protection officer on the other hand deprives each of these three services

of any possibility of independent control by the data protection officer. In addition,

the combination of these functions may have the effect that secrecy and confidentiality towards the

members of staff, under Article 38.5 of the GDPR, cannot be sufficiently

guaranteed.

67. The Respondent attempts to refute the existence of a conflict of interest on the part of the Chief

data protection by affirming that the MRI, ORM and IUS services are part of the function of

second line and only include monitoring and control functions. According to

defendant, the head of these services, who is also a data protection officer, did not

of decision-making competence in terms of the purposes and means of the operational processing of

personal data, but only an advisory and control competence. For

this argument, the Respondent believes that it finds support in the decision on the merits

No. 56/2021 of April 26, 2021.

68. As already defined in the Group Guidelines 29 concerning delegates to the

data protection12, the Litigation Chamber considers that the assessment of any conflict

interest must be made on a case-by-case basis, given the specific structural organization of any

organization. The Litigation Chamber thus carries out an assessment in concreto.

69. Although the Respondent submits that the three services in question are part of the function of

second line and therefore that these services do not introduce treatments themselves, but

limit to exercise supervision, establish frameworks and carry out controls, the Chamber

Contentious verifies during the hearing the relationship between the second line function and that of

first line in order to know if the second line function can carry out its task of advising and

control without defining the purpose and means of any own processing and processing

by the first line function. In concrete terms, the Litigation Chamber observes during

the hearing only when the second-line function must exercise its powers of control and

monitoring, it also needs information from the frontline function. That is what

also emerges from the register of processing activities in which a number of

important categories of personal data that are processed by the function of

second line. According to the Litigation Chamber, it clearly emerges that data to be

personal character are processed by the second line function for which it determines

the end and the means.

12 See footnote 11, above.

Decision on the merits 1412021 - 19/26

70. The Respondent's reaction in this regard is that the knowledge, namely the reading, of

personal data is not sufficient to qualify it as personal data processing.

personal character. The defendant thus makes a comparison with a worker who consults the

personal data in the context of his work, but does not himself act as

as a separate controller. Following another interpretation would result, depending on the

defendant, that each worker must be considered as separately responsible for the

treatment.

71. With regard to the categories of personal data set out in the register of

treatment which are processed by the second line function, the respondent asserts that these

are stated as a 'caution', because the second-line function may become aware

of this personal data for the performance of its tasks. The defendant adds

new that the second line function does not have the responsibility for the processing of data

personal nature, but that it can take cognizance of certain categories of data

personal character only through the exercise of its control competence and that the function

second line can never determine how personal data will be

interpreted and processed within the bank.

72. The Litigation Chamber points out that the consultation of personal data

does constitute processing within the meaning of Article 4, 2) of the GDPR. It should be specified at this

respect that the processing of personal data does not imply that the person carrying out the

treatment, such as a worker, must be qualified as a separate controller from the

treatment. The data controller is the one who determines the purposes and means of the

processing within the meaning of Article 4, 7) of the GDPR. The second-line function participates in the

determination – as an entity within the controller – of the purpose and means

with regard to the personal data that the first-line function must

provide – and thus participates in this sense in determining the purpose and means of processing

of the Front Line Service – so that the second line function can ensure its own

control and advice. This is undeniably apparent from the processing register. It results

that the Data Protection Officer, who also has the function of Head of Services

ORM/IRM/SIU, determines the purpose and means of data processing by the

first line insofar as this information is necessary for the tasks whose function

of the second line has been charged and that he then also defines the purpose and the means of the

data processing that the second line function performs.

73. This leads the Litigation Chamber to the conclusion that the combination of the quality of delegate to

data protection with the function of head of service of the three ORM/IRM/SIU services is not

not defensible without a conflict of interest on the part of the data protection officer.

The Litigation Chamber therefore considers that the violation of Article 38.6 of the GDPR is proven.

Decision on the merits 1412021 - 20/26

74. It is important that the data protection officer be able to carry out his missions and tasks in

compliance with the position as Article 38 of the GDPR has attributed to it, in particular that it can

intervene without there being a conflict of interest. The Litigation Chamber therefore instructs the defendant to

to bring the processing into compliance with article 38.6 of the GDPR on this point and thus to ensure that

that these missions and tasks do not entail any conflict of interest.

75. Considering the fact that the GDPR has given a key role to the data protection officer in

assigning an informative and advisory mission with regard to the controller

regarding all matters relating to the protection of personal data, including

notification of data breaches, the Litigation Chamber also imposes

an administrative fine.

76. In addition to the corrective measure to bring the processing into compliance with Article 38.6 of the GDPR,

the Litigation Chamber also decides to impose an administrative fine whose purpose is not

not to put an end to an offense committed but to effectively enforce the rules of the

GDPR. As can be seen from recital 148, the idea pursued by the GDPR is that in the event of

serious violations, sanctions, including administrative fines, are imposed, in

complement or instead of the appropriate measures that are imposed.13 The Litigation Chamber

does so pursuant to Article 58.2(i) of the GDPR. The instrument of the administrative fine has not

therefore in no way intended to put an end to the violations. To this end, the GDPR and the LCA provide

several corrective measures, including the orders cited in Article 100, § 1, 8° and 9° of the LCA.

77. First, the nature and gravity of the violation are taken into account by the Chamber

Litigation in order to justify the imposition of this sanction and the extent of it.

78. In this context, the Litigation Division finds that although there is no element revealing that there

either a question of an intentional violation, it is a serious breach on the part of the

respondent. Although the Data Protection Officer is a prescribed function

mandatory for the first time at European level in the GDPR, the concept of a delegate to

data protection is not new and has existed for a long time in many states

members and in many organizations.14

13 Recital 148 provides the following: "In order to strengthen the application of the rules of this Regulation, sanctions including

administrative fines should be imposed for any violation of this Regulation, in addition to or instead of the

appropriate measures imposed by the supervisory authority under this Regulation. In the event of a minor violation or if the fine

liable to be imposed constitutes a disproportionate burden for a natural person, a warning may be issued

rather than a fine. However, due consideration should be given to the nature, gravity and duration of the breach, the character

intent of the breach and the measures taken to mitigate the damage suffered, the degree of responsibility or any breach

relevant previously committed, the manner in which the supervisory authority became aware of the breach, compliance with

measures ordered against the controller or processor, the application of a code of conduct, and any

other aggravating or mitigating circumstance. The application of sanctions, including administrative fines, should be subject to

appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including the right to

effective judicial protection and due process.

14 See in particular WP243Rev01, paragraph 1.

Decision on the merits 1412021 - 21/26

79. In addition, Group 29 has already established guidelines for these delegates on December 13, 2016.

These guidelines were revised on April 5, 2017 after extensive public consultation. As

As can be seen from the following, these guidelines are clear regarding the extent to which the

data protection officer may also perform other functions within

company, taking into account the organizational structure specific to each body, and this

aspect must be considered on a case-by-case basis.

80. In short, according to the Litigation Chamber, there is no doubt as to the fact that the accumulation of the

function of data protection officer with a function as head of a

department (in which personal data is also processed) that the

data protection officer must control cannot take place independently.

81. An organization such as the Respondent can be expected to prepare conscientiously

the introduction of the GDPR and this from its entry into force, in accordance with article 99 of the GDPR in

May 2016. The processing of personal data is indeed a central activity

of the defendant, who also processes data on a very large scale.

82. The duration of the infringement is also taken into account. The delegate for the protection of

data was created by the GDPR, which has applied since May 25, 2018, so that the violation of

Article 38.6 of the GDPR is already established from this date. In any event, the infringement lasted

until the date of entry into service of the full-time Data Protection Officer,

i.e. July 1, 2021.

83. Finally, the defendant processes personal data of a very large number of people.

Ineffective safeguards for the protection of personal data, more specifically

by appointing a data protection officer who does not meet the independence requirement

and therefore cannot operate without a conflict of interest, therefore have a potential impact on a number

huge number of people involved.

84. All of the elements set out above justify an effective, proportionate and

dissuasive, as referred to in Article 83 of the GDPR, taking into account the assessment criteria that it

contains, up to an amount of 75,000 euros. The Litigation Chamber draws attention

on the fact that the other criteria of Article 83.2 of the GDPR are not, in this case, such as to

lead to an administrative fine other than that defined by the Litigation Chamber in the

framework of this decision.

85. When determining the amount of the administrative fine, the Litigation Chamber takes

into consideration the mitigating circumstances to which the defendant refers in its reaction

for the Litigation Chamber to impose an administrative fine, namely the absence

damage to data subjects (Article 83.2 a) of the GDPR); the measures taken to

detect in good time and prevent a potential conflict of interest, in particular by setting up

Decision on the merits 1412021 - 22/26

appropriate policies and mechanisms as described in the conclusions (article 83.2, c) of the

GDPR); the absence of previous relevant violations (Article 83.2 e) of the GDPR), as well as the

good faith collaboration with the DPA (article 83.2 f) of the GDPR).

86. To respond concretely to the Respondent's objection, the Litigation Division asserts that it has not

certainly not found that there was any question of damage on the part of the persons concerned,

but the absence of any damage has also not been demonstrated, and violations have not been

observed previously. This finding led the Litigation Division to reduce the amount

initially envisaged from the administrative fine, namely EUR 100,000, to EUR 75,000.

87. With regard to the implementation of policies and mechanisms intended to avoid conflicts

interest, the Litigation Chamber points out that these were taken late, that is to say

well after the entry into force15 and application16 of the GDPR. The 'Conflicts of Interest Policy' dates

of January 20, 2020 and the policy specific to the DPO was implemented on October 12, 2020 following

to decision on the merits No 18/2020 of 28 April 2020, as indicated in the conclusions, and a

full-time data protection officer was only appointed on July 1, 2021. This means

that the Respondent certainly cooperated with the DPA to remedy the violation and limit its

possible negative effects, but this occurred long after the entry into force and the implementation

application of the GDPR, which has an impact on the duration of the breach (see point 82 above).

88. With regard to the amount of the fine, the defendant objects that the fine is higher than

that imposed for an identical violation in decision on the merits No 18/2020 of the

April 28, 2020, while the defendant claims that its consolidated turnover is lower, that it

has already taken steps to address ODA concerns and has a lesser position

on the market.

89. The Litigation Chamber declares that the maximum amount of the administrative fine for a

violation of Article 38 of the GDPR is defined in Article 83.4 of the GDPR17. The amount of the fine

imposed in this Decision is significantly lower than the maximum amount defined in Article

83.4 of the GDPR, given that the Litigation Chamber took into consideration all the

criteria set out in article 83.2 of the GDPR. In addition, the Litigation Chamber assesses the elements

concrete facts of each file separately in order to impose an appropriate sanction18.

15 Pursuant to Article 99.1 of the GDPR, the GDPR entered into force on May 25, 2016.

16 Article 99.2 of the GDPR states that the GDPR is applicable from May 25, 2018.

17 Article 83.4 GDPR. Violations of the following provisions are subject, in accordance with paragraph 2, to fines

administrative costs of up to EUR 10,000,000 or, in the case of a company, up to 2% of annual turnover

total worldwide for the previous financial year, whichever is higher:

the obligations of the controller and processor under Articles 8, 11, 25 to 39, 42 and 43;

has)

[…]

18 See in this respect the judgment of the Cour des marchés of July 7, 2021, roll number 2021/AR/320, NV Nationale Dienst voo

van Kinderartikelen (N.D.P.K. N.V.) c. ODA, p. 42

Decision on the merits 1412021 - 23/26

Respondent's reference to Decision on the Merits No. 18/2020 of April 28, 2020 concerns the

same violation, namely the existence of a conflict of interest on the part of the Data Protection Officer

data (article 38.6 of the GDPR) but for the rest, the Litigation Chamber must take into account

of all the factual elements specific to each separate file. In this case, the duration of

the violation constitutes an important element, which in this case justifies a fine of EUR 75,000,

for which the Litigation Chamber bases itself on the defendant's consolidated annual accounts.

d) Register of processing activities (Article 30 of the GDPR)

90. With regard to the register of processing activities, the Inspection Service makes the findings

following, as summarized below:

-

-

the register of processing activities of the ORM/IRM/SIU services19 is incomplete;

the register of processing activities only includes three processing activities, namely

a single processing activity for each of the services. The Inspection Service finds this

strange, given that in each of the three services there are different activities of

treatment within the second line function and therefore it is rather abnormal to resume

these processing activities under a single processing activity;

-

the respondent has not provided a complete enumeration of all the purposes for processing the

personal data, in accordance with Article 30.1 b) of the GDPR;

-

the following information from the record of processing activities is not visible:

•

the name and contact details of the data protection officer, in accordance with

GDPR Article 30.1(a);

• a description of the envisaged timeframes within which the different categories of

data must be erased, in accordance with Article 30.1 f) of the GDPR;

• a description of the technical and organizational security measures,

in accordance with Article 30.1 g) of the GDPR.

-

the record of processing activities itself must be complete and clear, but the terms

are not explained: "12. TIN" and "S9. Criminal data". The description of the purposes of the

treatment is also vague: "E7_To support the activities to safeguard and ensure the

security and integrity of Y and/or the financial sector" and "C6_Compliance with legal

obligations", and does not accurately reflect the processing activity and the purpose of the processing

of these services of the defendant.

19 Operational Risk Management (ORM)/Information Risk Management (IRM)/Special Investigation Unit (SIU).

Decision on the merits 1412021 - 24/26

-

specifically for the SIU service, the record of processing activities mentions that the

personal data relating to criminal convictions and offenses are

treated with the following mention "S9. Criminal data". The Inspection Service finds it strange

that is not specifically explained.

91. The Respondent submits the following with respect to these findings of the Inspection Service:

- Except for the list of elements which must be included in the register and

the obligation to communicate the register to the supervisory authority upon request, the GDPR does not impose

no other legal obligation regarding the register. According to the respondent, the Service

of Inspection therefore seems, by its findings in the inspection report, to want to place the

bar higher than the legal requirements in this area. The defendant adds and demonstrates that he has

also taking into account recommendation no. 06/2017 of June 14, 2017, as formulated by

the Privacy Commission;

- Regarding the vague terms and the vague description of the purposes of the processing, the

defendant asserts that the register is an internal instrument and an aid for the person in charge of the

treatment. The defendant acknowledges that the register also serves as a source of information for

ODA and that in this sense it must also be understandable for ODA itself. It is not

however, it cannot be ruled out that the controller may still provide explanations to

the DPA for certain internal terminologies used in the registry. GDPR Article 30.1

requires that the register of processing activities include a description of the categories of

personal data, as well as the purposes of processing, but does not include

concrete obligation as to the level of detail of these categories of personal data

personal and processing purposes. In the aforementioned Recommendation No. 06/2017, it is

also gives examples of categories of personal data and purposes

which are of the same "general" nature.

With regard to the concepts and purposes that the Inspection Service describes as vague, the

Respondent asserts that these were defined in another internal document. The definitions

of this document – both as regards the categories of personal data and

the purposes – were included in the register and were already available in the register in

clicking on the terms in question.

- The defendant emphasizes that the Inspection Service only requested the register of the activities of

treatment of ORM/MRI/IUS services and not the full registry. The document provided by the

defendant was a limited extract from the register and includes only details of the activities

processing of the services concerned.

- The processing activities of the ORM, MRI and SIU services are further explained by the

respondent. He states that the IRM and ORM services are primarily advisory and

control, without actually having an execution task at the information processing level

and/or personal data. These are very limited treatments that are grouped

in the register under a single processing activity for each of the two services. Some

number of processing activities that the Inspection Service assigns respectively to the

MRI service and ORM service are activities that are described elsewhere in the register for

the sections responsible for it. With regard to the SIU service, the activities are

also described and here too they have been taken together in the extract from the

register as a single processing activity. The Respondent again emphasizes that the

GDPR does not provide any specific level of detail required.

- With regard to the information which, according to the inspection report, is missing in the

record of processing activities, the respondent argues that the name and contact details of the

data protection officer are included in a large number of internal documents

and are therefore well known within the defendant's organization, but that this data

concerning the data protection officer do not appear in the extract from the register

processing activities for purely technical reasons.

With regard to retention periods, as well as technical and

organisational, Article 30 of the GDPR requires that the register contain this information in

as far as possible, but does not as such require them to be mentioned in the register

well said. The respondent asserts that it was decided to describe this information in

separate documents for pragmatic reasons and for greater clarity.

92. On the basis of the defense and the supporting documents, the Litigation Chamber decides that in the

on the part of the defendant, there is no violation of Article 30 of the GDPR.

III. Publication of the decision

93. Seen

the importance of

transparency regarding

the decision-making process of

bedroom

Litigation, this decision is published on the website of the Authority for the protection of

data. However, it is not necessary for this purpose that the identification data of the parties

are communicated directly.

Decision on the merits 1412021 - 26/26

FOR THESE REASONS,

the Litigation Chamber of the Data Protection Authority decides, after deliberation:

-

pursuant to Article 100, § 1, 5° of the LCA, to order a dismissal for the violation of Articles 5.1

d), 16 and 25 GDPR;

-

pursuant to Article 100, § 1, 13° and Article 101 of the LCA, to impose an administrative fine

of €75,000 following the violation of article 38.6 of the GDPR.

Pursuant to Article 108, § 1 of the LCA, this decision may be appealed to the Court

contracts within thirty days of its notification, with the Protection Authority

data as a defendant.

(Sr.) Hielke Hijmans

President of the Litigation Chamber