Litigation Chamber

Decision on the merits 18/2020 of 28 April 2020

File number: AH-2019-0013

Subject: Inspection report relating to the responsibility for data leaks and the

position of the data protection officer

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

Hijmans, chairman, and Messrs. Dirk Van Der Kelen and Jelle Stassijns, members;

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

protection of natural persons with regard to the processing of personal data and the

free movement of such data, and repealing Directive 95/46/EC (General Regulation on the

data protection) (hereinafter the "GDPR");

Having regard to the law of 3 December 2017 establishing the Data Protection Authority, hereinafter the

"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;

Decision on the merits [number] / [year] - 2/20

made the following decision regarding:

Y, hereinafter "the defendant"

1. Facts and procedure

A. Investigation by the Inspection Service

On July 11, 2019, 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.

After examination of the file by the First Line Service, it turns out that three serious points

jeopardize proper compliance with the GDPR:

1.

2.

3.

failure to comply with the obligation to cooperate (Article 31 of the GDPR);

non-compliance with responsibility (Article 5.2 of the GDPR) and the obligation to cooperate

(Article 31 GDPR) regarding the application of the risk-based approach

("risk based approach") in the context of the security of personal data

(Article 36 of the GDPR);

failure to comply with the defendant's obligation to avoid a conflict of interest on the part of the

data protection officer (article 38.6 of the GDPR) and the fact that the data protection officer

data protection is not sufficiently involved (Article 38.1 GDPR).

The reason for the aforementioned referral was a concrete leak of data at the level of the defendant.

This leak was also referred to as Incident W. This data leak took place as part of

several invitations which were sent by the defendant in particular to freelancers and

people exercising a liberal profession in order to switch from paper invoicing to invoicing

electronic. Following an error in the selection of e-mail addresses, several invitations linked to

persons exercising a liberal profession and to the self-employed (and then also the invoice

email) were sent to linked secondary email addresses in the databases of the

defendant, to a client but potentially having no direct link with the client concerned.

These secondary contact persons are administrative or technical contact persons

to the customer.

The communications carried out around this data leak between the Front Line Service of

the DPA and the defendant gave rise to a note submitted by the Service de Première Ligne to the Committee

direction, containing a proposal to assess the existence of serious indications and then submit

the file to the Inspection Service in order to have the defendant's handling of the leaks examined

of data (article 63, 1° of the LCA).

The Inspection Department sent its report of September 6, 2019 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

In the session of September 24, 2019, the Litigation Chamber decided, pursuant to Article 95, § 1, 1° of the LCA, that the case could be dealt with on the merits.

On the same day, the defendant was 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. Similarly, the Respondent was informed of the provisions of Article 98 of the LCA and, pursuant to Article 99 of the LCA, he was informed of the deadlines for introducing its findings. The deadline for receipt of the respondent's submissions in response has been set to October 28, 2019.

On October 29, 2019, the Litigation Chamber received the submissions in response from the respondent. In addition to the substantial defense concerning the three findings of the Inspection Service relating to the obligation to cooperate (1), the liability of the controller (2) and the position of the data protection officer (3), these conclusions also contain a means of procedural defense in which the defendant objects that in this case, the distribution of competences delimited by the legislator between the Front Line Service and the Inspection Service was not respected, which would lead to the incompetence of the Litigation Chamber and to the inadmissibility of the report of the Inspection Service and the internal note of the Front Line Service.

On February 14, 2020, the processing of the file is resumed and the hearing takes place. The defendant is therefore heard and has the opportunity to present its arguments.

Then, the case is deliberated by the Litigation Chamber.

Pursuant to article 54 of the internal rules of the Data Protection Authority, a a copy of the minutes of the hearing is sent to the defendant on February 18, 2020.

The defendant is thus offered the opportunity to have any comments added in this regard.

appended to the minutes, without this implying a reopening of the debates.

On February 21, 2020, the Litigation Chamber receives from the defendant some remarks relating to the

minutes, remarks that it decides to include in its deliberation and in its decision.

Decision on the merits [number] / [year] - 4/20

On February 26, 2020, as requested during the hearing, the Respondent transmitted the

correct company number and annual turnover for the last three financial years This figure

of business is:

for 2017: €4,058,643,958

for 2018: €4,009,935,363

for 2019: €3,886,699,793.

On April 3, 2020, the Litigation Division informed the defendant 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 themselves before the sanction is actually imposed and carried out.

On April 24, 2020, the Litigation Chamber receives the defendant's reaction concerning the intention

to impose an administrative fine, together with the amount thereof. The defendant says he is not

agrees with the imposition of a fine or with the proposed amount of the fine and it refers to this

effect to its conclusions. However, he does not put forward any (new) argument to support this position.

Therefore, in the eyes of the Litigation Chamber, the defendant's reaction does not give rise to a

adaptation of the intention to impose an administrative fine, nor to a modification of the amount of

the fine as envisaged.

2. Legal basis

Article 38.6 GDPR

"6. The data protection officer may perform other tasks and tasks. The person responsible

of the processing or the processor ensure that these missions and tasks do not lead to any conflict

of interest."

3. Motivation

a) Procedure

As a first defence, the Respondent argues that the proceedings would present several

shortcomings. The defendant objects that the Front Line Service went further than simply

processing of the notification file, so that we no longer find any trace of the incident W

in the objections at the origin of the procedure before the Litigation Chamber. According to the defendant, he

emerges from the written request for information, specifically the scope of the questions and

Decision on the merits [number] / [year] - 5/20

the number of additional questions, which the Front Line Service conducted an investigation,

which, in accordance with Article 66, § 1, 3° of the LCA, falls within the investigative competence of the Service

of inspection.

The Front Line Service would also have used the survey modality to identify

persons, which falls within the competence of the Inspection Service (article 66, § 1, 1° of the LCA).

The Respondent asserts that its argument – that the investigation has already been conducted at the level of the

Front Line Service and therefore before the file reaches the Inspection Service – is

confirmed by the fact that for "investigative measures related to the investigation", the report of the Service

of Inspection refers exclusively to the "analysis of the file received via the Management Committee"

[Editor's note: all the passages from the inspection report are free translations made by the

Secretariat of the Data Protection Authority, in the absence of an official translation]. According to

respondent, the Inspection Service therefore bases its report simply and solely on an investigation

which was conducted by Front Line Service.

During the hearing, the defendant adds to this that the internal memo from the Service de Première

Line, which was addressed to the Management Committee and therefore at a time when the Inspection Service had not

not yet seized of the file, had already been sent with the mention of the coordinates of the Service

of Inspection (inspection@apd-gba.be). The carrying out of investigative actions by a service which cannot

not legally carry them out is qualified as a fishing expedition by the defendant.

According to the defendant, the Front Line Service therefore exceeded its jurisdiction and did not

not bound by its legal competences, more precisely its competence to launch a procedure of

mediation (article 22, 2° of the LCA). The respondent asserts that the Front Line Service did not

acceded to its multiple requests for consultation.

Furthermore, according to the defendant, the Inspection Service did not respect its powers either,

given that he relied exclusively on the file of the Front Line Service to draft the

report. This leads the defendant to assert that the Inspection Service did not carry out any investigation because

none of the investigative measures listed in Article 66, § 1 of the LCA have been taken. The defendant

argues that the Inspection Service was therefore not competent to draw up its report, given that it

could not lawfully close its investigation, due to the lack of any measure

of investigation.

The defendant asserts that the Litigation Chamber was not seized in a valid way in law and

must declare itself incompetent because:

-

-

the Inspection Service did not carry out any investigation;

the Inspection Service was not competent to close its investigation;

-

the Litigation Chamber could only be seized after a lawful closure of the investigation.

In the alternative, the defendant objects that the report of the Inspection Service and the internal note of the

Front Line Service cannot be admitted due to violation of legal principles

fundamental principles, in particular the principle of due process and the right of defence, as well as

general principles of good governance, within the framework of which the Litigation Chamber, in

as an administrative authority, must in particular respect the principles of precaution and

of impartiality.

During the hearing, the defendant does not deny that an investigation was carried out but he claims that it was done the wrong way. The defendant argues that the Litigation Chamber is not competent when the elements collected have been obtained in a legally incorrect manner. According to the defendant, the documents of the Front Line Service must therefore be excluded from the investigation and he stresses that the Front Line Service must intervene within the framework of its competences as defined in Article 22 of the LCA. According to the Respondent, compliance with this principle is essential for legal certainty. The defendant explicitly asserts that he is important for a company to be able to dialogue with a department within the APD without a investigation is carried out from the outset, in such a way as to allow collaboration, consultation and mediation.

The Litigation Chamber emphasizes that impartial and fair treatment must be ensured throughout the journey. The problem raised by the Respondent concerns the preliminary phase, but the rights of the defense were not violated, because the defendant had the opportunity to put forward his case in its entirety by means of its submissions in response and it was furthermore able to fully exercise its right to contradict during the hearing of the Litigation Chamber.

The Litigation Chamber can only note that in the event that the DPA can intervene ex officio, the procedure provided for by law has been complied with, namely that when the Management Committee observes serious indications of the existence of a practice likely to give rise to an infringement of the fundamental principles of the protection of personal data, within the framework of the LCA and laws containing provisions relating to the protection of the processing of personal data staff, referral to the Inspection Service may take place (article 63, 1° of the LCA). In application of the foregoing, pursuant to the decision of the Management Committee taken on July 11, 2019, the Service of Inspection was seized of the file on August 12, 2019, without a rule of procedure which would be of such a nature to harm the defendant's interests or violate his rights is violated. The procedural guarantee fundamental principle of ensuring the right to contradict has been respected given that the report of inspection was sent by the Litigation Chamber to the defendant and that he had the opportunity to react to each of the findings made by the Inspection Service in this report.

The Litigation Chamber therefore considers that this notification of a possible breach of
personal data has been processed in compliance with all principles of law
fundamentals and general principles of good governance.

b) Cooperation with the supervisory authority (Article 31 GDPR)

With regard to the obligation to cooperate, the Inspection Service establishes the following observation in
his report :

“The defendant used different means to complicate the obligatory cooperation with the DPA.
These means are described on the Internet pages http://www.aalep.eu/recognizing-your-opposition-
tactics-and-responding-them and https://ctb.ku.edu/en/table-of-contents/advocacy/respond-to-
counterattacks/overview-of-opposition-tactics/main as the “Ten D's”.
As part of an assessment of contact with the respondent, it may be found that the respondent
applied 5 of the 10 techniques.
According to the Inspection Service, it is up to the Litigation Chamber to establish whether the application of
aforementioned techniques constitutes a breach of the obligation to cooperate or may be
considered as a normal exercise of the defendant's right of defense on the basis of the principles
applicable general laws.”

Regarding these findings of the Inspection Service in terms of cooperation, the Respondent submits
first of all that since the Front Line Service exceeded its competence and therefore did not
fulfilled the missions assigned to him, he was not to cooperate and was not to have access to
Front Line Service requests. Second, the defendant disputes the legal value of the
Internet pages on which the APD relies and he argues that he did cooperate
and did not apply any of the five "Ten D's" techniques. The respondent asserts that the requirement of
cooperation is in any case limited by the right of defense and the right not to incriminate oneself
oneself, which applies in administrative procedures that may give rise to the imposition
administrative fines. Extensive questioning would violate the right of defense and

prohibition of self-incrimination.

The Litigation Chamber assessed the findings of the Inspection Service in the light of the obligation

of cooperation from the defendant and finds that the Inspection Service has not demonstrated sufficiently

that the defendant had not attempted through response letters to respond in detail

and detailed to the questions asked. In addition, the defendant repeatedly declared himself

willing to engage in consultation, in addition to this approach. We therefore cannot establish

Decision on the merits [number] / [year] - 8/20

that he did not take into account the obligation to cooperate with the supervisory authority.

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 unnecessary.

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

c) Liability (Article 5.2 GDPR and Article 24(1) GDPR) with respect to

concerns the application of risk assessment when notifying a breach of

personal data (Article 33 GDPR)

Regarding these serious indications from the Management Committee, the inspection report mentions the

following finding:

“The respondent's risk assessment when notifying data breaches

staff was consistently "low" or "negligibly low" over the past year.

The manner in which the defendant's team (composed of business representatives) arrived at this

result, despite the questions posed in this respect by the APD, is not concretely clear. Like this

appears from the defendant's letter of 06/12/2019, he is not prepared to explain this aspect further

because it would not be required to do so under the GDPR. It also emerges from the "RACI matrix" referred to in the

aforementioned letter that the data protection officer of the defendant does not participate in the

discussions relating to the risk assessment in this matter since it is only

"informed" rather than "consulted". Who decides what within the defendant in a concrete file is not

not communicated to the DPA and there is no indication that the Respondent wishes to modify

this practice.

Due to the use of vague descriptions of the evaluation process and negations, it is

impossible for the DPA to verify the manner in which the defendant arrives at a certain conclusion in

risk in a specific file.

The above-mentioned method is contrary to liability (Art. 5(2) GDPR) and to the

liability (Art. 24 (1) GDPR) of the defendant with regard to the application of

the risk-based approach to personal data security

(Article 32 of the GDPR)."

The respondent points out that the inspection report only explicitly refers to the approach

based on the risks in the context of the security of personal data (Article 32 of the

GDPR) while it appears from the content of the report that it is about the risk assessment during the

notification of personal data breaches, which concerns Articles 33 and 34 of the

GDPR, thus making it impossible for the defendant to properly defend himself, which involves

Decision on the merits [number] / [year] - 9/20

consequences for the decision of the Litigation Chamber from the point of view of the principles of law

fundamentals and general principles of good governance.

On this point, the Litigation Division considers that, disregarding this finding by the defendant

concerning the applicable articles of law, the conclusions of the defendant do not contain the slightest

element revealing that he also defends himself concerning the risk-based approach within the framework of the

security of personal data (Article 32 of the GDPR). Integral defense concerns

risk assessment when notifying personal data breaches

(Articles 33 and 34 of the GDPR). There is nothing to show that on the part of the defendant there was the

slightest doubt as to the articles at the origin of the finding of the Inspection Service, so that

on this basis, it must be concluded that the fundamental principles of law and the general principles

of good governance have been respected. This is explained by the fact that all the documents in the file

relate to risk assessment when notifying data breaches

staff. The inspection report also mentions at the beginning of the finding that this concerns

risk assessment when notifying personal data breaches and it

It is clear from the context of the report that it is just that.

In terms of content, the defendant asserts that there is no legal obligation to submit a

possibility of detailed verification at the APD. Information relating to the methodology for the analysis

risks and the procedure relating to this analysis and the decision-making process have indeed been

provided to ODA. Despite the challenge to the jurisdiction of the DPA, the Respondent points out that

information was nevertheless provided, in the context of which he indicated that he wanted to engage

dialogue on risk assessment. The respondent also reacts to the Service's position

of Inspection that by using vague descriptions of the assessment process and

denials, the Respondent prevents the DPA from verifying how the Respondent arrived at a

certain conclusion in a specific file.

The Respondent refers in its pleadings to the relevant exhibits which would invalidate this position

of the Inspection Service and which would thus allow the DPA to check how

the defendant has come to a certain conclusion regarding the risks in a concrete case.

The defendant concludes that there is no breach of liability, since Article 5.2 of the

GDPR would only concern the principles mentioned in article 5.1 of the GDPR and not the rules relating

the consequences of a personal data breach.

The Litigation Chamber emphasizes that contrary to what the defendant asserts, there is indeed

on the part of the data controller an obligation to document each data leak,

whether it involves risks or not, in order to be able to provide information to the DPA. In addition,

also contrary to what the defendant asserts, article 5.2 of the GDPR is not limited to the principles

listed in article 5.1 of the GDPR but does also concern the other provisions of the GDPR,

including Article 33 of the GDPR. This results from the close link between on the one hand article 5.2 of the GDPR and on the ot

part of the obligations for the controller arising from articles 24 and following of the

GDPR.

The Litigation Chamber refers to this effect to the Guidelines on the notification of violations of

personal data under Regulation 2016/679 of the Article 29 Working Party on the

data protection1 which specify the following:

“Whether a breach requires notification to the supervisory authority or not, the controller

is obliged to document all violations, as explained in Article 33, paragraph 5:

The data controller documents any breach of personal data, in

stating the facts about the personal data breach, its effects and the

measures taken to remedy it. The documentation thus compiled allows the supervisory authority

to verify compliance with this article.

This documentation obligation is linked to the principle of liability of the GDPR set out in

Article 5, paragraph 2. This requirement to keep records of violations, whether they are

subject to notification or not, is also linked to the obligations of the controller

under section 24, and the supervisory authority may request to see such records.

Controllers are therefore encouraged to establish an internal register of breaches,

whether they are required to notify them or not.

If it is up to the data controller to determine the method and structure to be used

to document a breach, certain key information should be included in all

circumstances. As required in Article 33(5), the controller must

resume information regarding the breach, including causes, facts and data

of a personal nature concerned. It should also include the effects and consequences of

the breach and the measures taken by the controller to remedy it.

The GDPR does not define the retention period for such documentation. When such

registers contain personal data, it will be the responsibility of the person responsible for the

processing to determine the appropriate retention period in accordance with the principles related

the processing of personal data and the legal basis for the processing. He will have to

keep this documentation in accordance with article 33, paragraph 5, as long as the authority
control could claim it as proof of compliance with said article, or more generally
of the principle of responsibility. Obviously, if the registers themselves do not contain
no personal data, the retention limitation principle of the GDPR does not
not apply.
1 WP250.Rev01, pp 30-32.

In addition to this information, the G29 recommends that the controller document
also the reasoning behind the decisions taken in response to the breach. Specifically,
where a breach is not notified, the rationale for this decision should be documented.
This justification should include the reasons why the controller
considers that the violation is unlikely to create a risk for the rights and freedoms of
people. If the controller considers that one of the conditions referred to in Article 34,
paragraph 3, is met, he should also be able to provide appropriate evidence
in this regard.
Where the controller does not notify a breach to the supervisory authority, but
notification is delayed, the controller must be able to provide the
reasons for such delay; documentation in this regard could help demonstrate that the
delay in notification is well justified and not excessive.
When the data controller communicates a violation to the data subjects, he
should be transparent about the violation in question and communicate in a
efficient and timely. Keeping track of such communication would thus help the
controller to demonstrate compliance with the principle of accountability and the GDPR by
general.
In order to promote their compliance with Articles 33 and 34, it would be beneficial both
for controllers and processors to have a procedure for

documented notification defining the procedure to be followed when a breach is detected, including

understood regarding how to contain, manage and remediate the incident, assess the risk

and notify the violation. In this regard, again in order to prove their compliance with the GDPR, it

may be useful to demonstrate that employees have been informed of the existence of such

mechanisms and procedures and that they know how to react in the event of a breach.

It should be noted that in the event of a breach of this obligation to properly document

breach, the supervisory authority could exercise its powers under Article 58 and/or

impose an administrative fine in accordance with Article 83." [underlining by the Chamber

Litigation].

In light of the aforementioned guidelines, the Litigation Chamber asked the defendant during

of the hearing to what extent he documented data leaks.

The respondent indicated that all known leaks were documented and that

this effect to the loyalty and professionalism of the individual worker in order to trace within

of the company a possible leak of data via the available tool. The defendant claims to have

necessary policies and organize training to educate its workers on the

notification of data incidents.

Decision on the merits [number] / [year] - 12/20

Considering these explanations provided during the hearing, as well as the fact that it appears from the documents in the file tha

the respondent, despite its challenge to the jurisdiction of the DPA to request information

detailed, agreed to the request to clarify the evaluation process in order to allow the DPA to

check how the defendant arrived at a certain risk conclusion

in a concrete file, namely incident W, the Litigation Chamber must conclude that the defendant

outlined its methodology and procedure for breaches and risk assessment.

The Litigation Chamber therefore considers that no violation of the

articles 5.2, 24.1 and 33 of the GDPR.

d) Position of the Data Protection Officer (Article 38 GDPR)

Regarding the position of the data protection officer, the report of the Inspection Service

makes the following findings:

In addition to this function, the data protection officer of the defendant also performs the

function of director of audit, risk and compliance with the defendant.

It emerges from this file that the Data Protection Officer is not in a position

sufficiently protected from a conflict of interest (as required by Article 38, paragraph 6 of the GDPR) and

that it is not sufficiently involved in discussions relating to data breaches

personal (as required by Article 38(1) GDPR).

Insufficient association of the Data Protection Officer

• The data protection officer of the defendant is only informed of the result of

risk assessment. In this regard, we refer to the letter of 06/12/2019 in

which the RACI matrix indicates in point 1.4.2.2 that its Data Protection Officer

is only "informed" and not "consulted". Article 38(1) GDPR requires

however, that the DPO be involved, in an appropriate and timely manner, in all

issues relating to the protection of personal data.

• The "DPO opinion" fields were until recently not systematically completed by

the defendant. It appears from the explanations given under point 1.4.2.2 of the defendant's letter

of 12/06/2019 (Exhibit 13) that the discussion relating to risk belongs to the "business" (which

is also apparent from the aforementioned RACI matrix) and that until recently the opinion of the

data protection officer was not included in the defendant's standard form

(“Personal Data Breach Investigation Report”).

Conflict of interest of the Data Protection Officer

•

Conflicting tasks. The defendant asserts in his letters of 03/04/2019 and of

12/06/2019 that its data protection officer only has an advisory role and

cannot make decisions about the purposes and means of the processing, which is

also mentioned in the [Guidelines for Data Protection Officers

Group Data (DPD) 29].2 The existence of a conflict of interest is not, however, limited

in cases where a person determines the purposes and means of the processing. Conflicts

interest must always be assessed on a case-by-case basis. The aforementioned letter from the defendant

indicates that its data protection officer does more than advise internally the

defendant since this person carries out conflicting tasks within Y

(the defendant) which involve considerable operational responsibility for the

data processing processes that fall within the scope of audit, risk and compliance.

• Pragmatic approach in Germany and in the doctrine,3 which [...] refer to criteria

such as (1) whether there is self-control by an authoritative office holder

within the company, (2) the existence or not of internal rules for conflicts of interest, and

(3) assume significant operational responsibility with an impact on the data to be

personal character...

• Until recently, the Respondent had no policy to prevent conflicts of interest.

It is only after the registered letters of the APD of 04/03/2019 and 16/05/2019

questioning the position of the data protection officer that a document not

dated "Y (defendant) DPO Charter" was transmitted by defendant's letter of 06/12/2019,

document which still had to be placed on the agenda of the Audit and Compliance Committee in

July 2019 (as mentioned on page 6 of the aforementioned letter from the defendant).

The drafting of such a document does not imply that it has thus been sufficiently demonstrated that the

Data Protection Officer works independently.

Regarding the association of the data protection officer, it is emphasized in the defense

that the finding of the Inspection Service is based on a legal misinterpretation and

factual.

According to the Respondent, as set out in its pleadings, for the application of Article 38.1 of the GDPR,

it would suffice for the data protection officer to be informed, which constitutes an element of

association, but this provision does not impose a specific obligation to be consulted, unlike

as mentioned in the inspection report.

2 WP 243Rev01, pp 20-21.

3 Press release of the Bavarian supervisory authority of 20/10/2016 on an IT manager, published at the following link:

https://www.lda.bayern.de/media/pm2016 OS.pdf and commented on the following link: https://iapp.org/news/a/german-compan

fined-for-dpo-conflict-of-interest/ as well as the relevant doctrine (namely F. SCHRAM, De functionaris voor

gegevensbescherming, Cahier 2 Edition, Politeia, 2019, 119-121).

Decision on the merits [number] / [year] - 14/20

The Litigation Chamber considers that the defendant's point of view is not in accordance with the ratio legis

and is not a sensible interpretation of Article 38.1 of the GDPR which states that the delegate must be

"associated, in an appropriate and timely manner, with all questions relating to the protection

personal data". Reduce the association of the data protection officer to

its simple information (a posteriori) concerning a decision empties its function of its content.

In this regard, the Litigation Chamber refers in particular to the Group 29 Guidelines for

data protection officers4, who stress that it is essential that the data protection officer

data protection is involved from the earliest possible stage in all matters relating to

to data protection. Ensure that the Data Protection Officer is informed and,

more importantly, being consulted from the start allows compliance with the General Regulation on the

Data protection.

In addition, it promotes adherence to a data protection by design approach, such as

than provided for in Article 25 of the GDPR and which must therefore be the usual procedure within the

governance of the organization.

The Litigation Chamber finds that the defendant misinterpreted Article 38.1 of the GDPR.

However, the Litigation Chamber considers that it has been made sufficiently plausible that with regard to

concerns the risk assessment process, the data protection officer is involved

in practice and conducts an independent privacy risk analysis itself,

before the final decision on the risks, by means of an opinion and its assistance as an adviser.

Regarding the outcome of the risk assessment, that a final decision has been taken by the

representatives within the team or department responsible for the affected services or customers, the

data protection officer is only informed, not consulted. This is in accordance with

Article 38.1 of the GDPR combined with Article 39.1.a) of the GDPR which requires that the data protection officer

data has an advisory role with respect to the data controller, but is not jointly responsible

of the final decision. On this basis, the Litigation Chamber confirms that the protection officer

of the data is only informed of the final risk decision.

4 "It is essential that the DPO, or his team, be involved from the earliest possible stage in all matters relating

to data protection. With regard to data protection impact assessments, the GDPR provides

expressly the involvement of the DPO at an early stage and specifies that the controller must seek advice from the

DPD when performing such an analysis. Informing and consulting the DPO from the outset will facilitate the

GDPR compliance and encourage a data protection by design approach; it should therefore be

standard procedure within the governance of the organization. Furthermore, it is important that the DPO be considered as a

interlocutor within the organization and that he is a member of the working groups devoted to data processing activities

within the organization.", WP24301Rev, paragraph 3.1 of the guidelines, underlining by the Litigation Chamber.

The Litigation Chamber concludes that on the one hand, the defendant has an erroneous interpretation of the

position of the data protection officer but that on the other hand, it is plausible that in the

practice, the data protection officer is sufficiently involved. Therefore, none

violation of Art. 38.1 GDPR cannot be established.

Regarding the finding of the Inspection Service that there is a conflict of interest

on the part of the Data Protection Officer due to the fact that he is also responsible

Compliance and Risk Management and Internal Audit, the Respondent argues that in

exercise of each of these functions, the person concerned does not take any decision

but that its role is purely advisory. Furthermore, the necessary measures would have been taken in

internally to avoid the risk of conflict of interest. These measures have been formalized in a DPO

Charter which was validated by the defendant's audit committee on July 29, 2019.

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. Regarding the role of the delegate

to data protection, the Litigation Chamber raises the question of how this

function is compatible with that of carrying out internal audits in the context of which

certain elements which may, where appropriate, give rise to the dismissal of a specific worker

can be compiled in a report. In this context, it is important to know whether the data protection officer

of data who also assumes the function of chief internal audit officer also has a right to

decision in this capacity.

The Litigation Chamber emphasizes that there is a difference between simple process analysis and

the evaluation of the functioning of the workers via an internal audit, which is in contradiction with

the function of trust that the data protection officer has within the company. In this

respect, the Respondent asserts that no compatibility issue arises given that as

as head of internal audit, the data protection officer concerned does not make any decisions

individual concerning the workers and does not evaluate them either.

The Litigation Chamber notes that in its conclusions, the defendant addresses in detail

the independence and advisory role of each of the three departments, namely the department

Compliance, the Internal Audit department and the Risk Management department, with respect to other

sections of the business. Thus, the defendant specifies that the Audit, Compliance and Risk roles do not involve

only limited risks of conflicts of interest because they have "advisory" functions and have no

decision-making authority regarding processing activities. This leads the defendant to assert

that the data protection officer has no task (not even via his functions in each

of the departments) where it could make decisions as to the ends and the means of the least

processing of personal data. 5

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

data, which is part of each of these departments and assumes a position of responsibility,

does not carry out any task that is incompatible with his position as delegate for the protection of

data.

The Litigation Chamber therefore points out that the independence and advisory role of the

department as such cannot be applied unconditionally to the person who fulfills

simultaneously the function of data protection officer and head of a department.

The Litigation Chamber must assess how and to what extent the independence of the

data protection officer is ensured vis-à-vis each of these three departments, in

particular in a situation like the present case where the data protection officer does not

only part of these departments but also assumes the role of manager of these

departments.

Indeed, the defendant explicitly stipulates that in addition to the responsibilities as delegate to the

data protection, the same person is also responsible for compliance, risk

management and internal audit.6 The defendant therefore himself designates the same natural person

as head of each of the three departments and as delegate for the protection of

data. 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 the field of compliance, risk management and audit

internally, as noted in the inspection report.

The Group 29 Guidelines for Data Protection Officers7 explain

that the data protection officer may not exercise a function within the organization which

5 Respondent's submissions, nos. 166 and 167.

6 See the letter of 3 April 2019 to the APD, cited in the conclusions.

7 "Article 38(6) allows DPOs to "carry out other duties and tasks". It does, however, require the body to ensure□

that "these missions and tasks do not involve a 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 provided that these do not give□

not give rise to a conflict of interest. This means in particular that the DPO may not exercise a function within the organization wh

leads it to determine the purposes and means of the processing of personal data. Due to the structure□

specific organizational structure of each organization, this aspect must be studied on a case-by-case basis.□

As a general rule, functions which may give rise to a conflict of interest within the organization may include:□

senior management functions (e.g. CEO, COO, CFO,□

chief medical officer, marketing department manager, human resources manager or service manager□

IT), but also other roles at a lower level of the organizational structure if these functions or roles require□

Decision on the merits [number] / [year] - 17/20□

leads it to determine the purposes and means of the processing of personal data.□

It is therefore a substantial conflict of interest. The role of head of a department is therefore not□

not reconcilable with the function of data protection officer who must be able to exercise his□

independent tasks. The accumulation, in the head of the same natural person, of the function□

responsible for each of the three departments in question separately on the one hand and□

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

of any possibility of independent control by the data protection officer. Furthermore, the□

accumulation of these functions may have the effect that secrecy and confidentiality towards the members of the□

personnel cannot be sufficiently guaranteed, in accordance with Article 38.5 of the GDPR.□

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

It is important that the data protection officer be able to carry out his missions and tasks within the□

compliance with the position assigned to it by Article 38 of the GDPR, 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□

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

Given 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 data controller concerning

all questions relating to the protection of personal data, including the notification

data breaches, the Litigation Chamber also imposes a fine

administration.

In addition to the corrective measure aimed at bringing 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

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 GDPR wants sanctions, including fines

administrative, be imposed in the event of serious violations, in addition to or instead of

the determination of the purposes and means of the processing. In addition, there may also be a conflict of interest, for example

if an external DPO is called upon to represent the controller or the processor before the courts in

cases relating to data protection issues.

Depending on the activities, size and structure of the organization, it may be good practice for those responsible for the

processing or subcontractors:

• to identify the functions which would be incompatible with that of DPD;

• establish internal rules to this effect, in order to avoid conflicts of interest;

• include a more general explanation regarding conflicts of interest;

• to declare that their DPO has no conflict of interest with regard to their role as DPO, with the aim of better

know this requirement;

• to provide guarantees in the organization's internal regulations, and to ensure that the vacancy notice for the position

of DPD or the service contract is sufficiently precise and detailed to avoid any conflict of interest. In this context,

it should also be borne in mind that 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.

appropriate measures that are imposed8. The Litigation Chamber thus acts pursuant to

Article 58.2.i) of the GDPR. The instrument of the administrative fine is therefore in no way intended to

put an end to violations. To this end, the GDPR and the LCA provide for several corrective measures, including

the orders cited in article 100, § 1, 8° and 9° of the LCA.

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.

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

whether a question of an intentional violation, it is a serious breach on the part of the defendant.

Although the Data Protection Officer is a mandatorily prescribed function for the

first time at European level in the GDPR, the concept of a Data Protection Officer

is not new and has existed for a long time in many Member States and in many

many organizations.9

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. Like him

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

data protection officer may also perform other functions within the company,

taking into account the organizational structure specific to each organization and this aspect must be

studied on a case-by-case basis.

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

that the data protection officer must check cannot take place in a way

independent.

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

the introduction of the GDPR as soon as the GDPR comes into force, in accordance with Article 99 of the GDPR

in May 2016. The processing of personal data is indeed an essential activity

8 Recital 148 provides the following: "In order to reinforce the application of the rules of this Regulation, penalties
including administrative fines should be imposed for any violation of this Regulation, in addition to or
instead of appropriate measures imposed by the supervisory authority under this Regulation. In the event of a minor violation
or if the fine that may be imposed constitutes a disproportionate burden for a natural person, a reminder to
the order can be addressed rather than a fine. However, due consideration should be given to the nature, seriousness and
the duration of the violation, the intentional nature of the violation and the measures taken to mitigate the damage suffered, the
degree of responsibility or any relevant violation committed previously, of the manner in which the supervisory authority had
knowledge of the breach, compliance with the 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 principles
principles of Union law and the Charter, including the right to effective judicial protection and to due process
regular."

9 See in particular WP243Rev01, paragraph 1.

of the defendant, who also processes personal data on a very large scale, including
personal data which may be of a very sensitive nature, in particular because
that they allow regular and systematic observation.10

The duration of the infringement is also taken into account. The data protection officer
was created by the GDPR, which has applied since May 25, 2018, so the violation of Article 38.6
of the GDPR is already established from this date. Be that as it may, the infringement still persisted at the
date of the hearing, i.e. February 14, 2020.

Finally, the defendant processes personal data of millions of people. Guarantees
ineffective for the protection of personal data, more specifically by designating a
data protection officer who does not meet the requirement of independence and therefore cannot
not intervene without conflict of interest, therefore have a potential impact on millions of people
concerned.

All of the elements set out above justify an effective, proportionate and dissuasive sanction,

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

up to an amount of 50,000 euros. The Litigation Chamber draws attention to the fact that

the other criteria of article 83.2 of the GDPR are not, in this case, likely to lead to another

administrative fine than that defined by the Litigation Chamber within the framework of this

decision.

e) Publication of the decision

Given the importance of transparency concerning the decision-making process of the Litigation Chamber,

this decision is published on the website of the Data Protection Authority. However, he

it is not necessary for this purpose that the identification data of the parties be directly

communicated.

FOR THESE REASONS,

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

- pursuant to Article 100, § 1, 9° of the LCA, to order the defendant that the processing be

brought into compliance with article 38.6 of the GDPR. To this end, the Litigation Division grants the

10 See in particular Article 37.1 of the GDPR. See in this respect also the case law of the European Court of Justice

regarding the potentially sensitive nature of telecommunications data, e.g. joined cases

C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others, ECLI:EU:C:2014:238, paragraph 37.

defendant within three months and expects the defendant to report to him no later than

July 31, 2020 concerning the compliance of the processing with the aforementioned provisions;

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

administrative amount of 50,000 euros.

Under article 108, § 1 of the LCA, this decision may be appealed within a period of

thirty days, from the notification, to the Court of Markets, with the Authority for the Protection of

given as defendant.

(Sr.) Hielke Hijmans

President of the Litigation Chamber