

Litigation Chamber

Decision on the merits 34/2020 of 23 June 2020

File number: DOS-2019-02426

Subject: processing of personal data included in the Crossroads Bank

cars

the Data Protection Authority, made up of

The Litigation Chamber of

Mr Hielke Hijmans, Chairman, and Messrs Frank De Smet and Dirk Van Der Kelen, 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

ACL;

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 34/2020 - 2/35

made the following decision regarding:

-

the Federal Public Service Mobility and Transport, City Atrium, rue du Progrès 56 - 1210

Brussels, whose company number is 0308.357.852, hereinafter "the defendant".

1. Facts and procedure

1. On April 3, 2019, the Board of Directors of the Data Protection Authority decides,

pursuant to Article 63, 1° of the LCA, to seize the Inspection Service of a file because it has noted serious indications indicating that certain insurance companies have access to personal data included in the Crossroads Bank for Vehicles and that this access would be used with a view to re-using this personal data for the purposes commercial. More precisely, these insurance companies would obtain this access via the Informex SA information platform.

2. On May 3, 2019, pursuant to Article 66, § 1 of the LCA, the Inspection Service sent a letter to the defendant, who is the controller of the personal data taken up in the Crossroads Bank for Vehicles, in which he asks him several questions:

1. "Since when have you been aware of the aforementioned practice of Informex SA (please attach a copy of correspondence and supporting documents)? Since when did your is the data protection officer aware of it (please attach a copy of the vouchers) ?

2. What concrete steps have been taken since you became aware of the practice aforementioned of Informex SA (please attach relevant documents in this regard which support your approach)? What was the opinion of your protection officer on this subject? data (please attach a copy of this notice)?

3. How do you assess the purpose limitation and legality of the practice of systematic reuse of BCV personal data by Informex SA via its platform www.audagarage.com for the benefit of various insurers for the online establishment of a premium proposal, given the BCV1 law and its decrees of execution and having regard to the privacy statement of the Federal Public Service Mobility and Transport on the website <https://mobilit.belgium.be/fr/privacy>?

4. Who is your Data Protection Officer, since when and how Was this choice justified in practice? Has your data protection officer been notified to the DPA? Can you document his duties, including any duties

1 Law of 19 May 2010 creating the Crossroads Bank for Vehicles, M.B. of 28 June 2010.□

Decision on the merits 34/2020 - 3/35□

unrelated to data protection, and its precise position in the organization chart of□

your organization with relevant documents?□

5. Do you qualify the aforementioned Informex SA practice as a data breach?□

personal character? Why or why not ? And if so, why no□

notification has yet been made to the DPA?"□

3. By letter dated May 29, 2019, the Respondent responds to these questions from the Inspection Service.□

4. By letter dated June 6, 2019, the Inspection Service sends the defendant its findings□

provisional as well as several supplementary questions.□

5. On August 19, 2019, the Inspection Service sends its inspection report to the Chairman of the□

Litigation Chamber, in accordance with Article 91, § 2 of the LCA, following which the Chamber□

Litigation is seized in accordance with article 92, 3° of the LCA.□

In its report, in the context of serious indications, the Inspection Service formulates□

findings regarding:□

-

-

compliance with the limitation of purposes (Article 5.1 b) of the GDPR) and the lawfulness of the□

processing (Article 6.1 of the GDPR) as well as□

compliance with the responsibility of the data controller (article 24 of the GDPR),□

the security of the processing (article 32 of the GDPR) and the notification to the authority of□

control of a personal data breach (Article 33 of the GDPR).□

In addition, the Inspection Service makes several additional findings apart from□

the framework of serious indications, namely concerning:□

-

-

•□

compliance with the provisions relating to the appointment of a data protection officer□

(article 37 of the GDPR) and the function of the data protection officer□

data (Article 38 GDPR);□

compliance with the obligation to cooperate (Article 31 of the GDPR and Article 66.2 of the□

ACL); and□

compliance with the obligation of transparency (Article 12 of the GDPR) and information□

to be provided (Article 13 of the GDPR).□

6. On September 24, 2019, the Litigation Chamber decides, pursuant to Article 95, § 1, 1° and□

of article 98 of the LCA, that the case can be dealt with on the merits.□

Decision on the merits 34/2020 - 4/35□

7. By registered letter of September 24, 2019, the respondent is informed that the complaint□

may be dealt with on the merits and, under Article 99 of the LCA, it is also informed of the□

deadline for presenting its conclusions.□

8. On October 28, 2019, the Respondent files its conclusions and requests to be heard,□

in accordance with article 98, 2° of the LCA.□

9. On May 4, 2020, the defendant was heard by the Litigation Chamber, in accordance with article□

53 of the internal rules.□

10. On May 6, 2020, the minutes of the hearing are sent to the defendant, in accordance with Article□

54 of the internal rules.□

11. On May 15, 2020, the Respondent transmits its remarks, which are annexed to the minutes□

hearing, in accordance with Article 54, second paragraph of the internal rules.□

2. Legal basis□

Article 5.1.b) GDPR□

1. Personal data must be: (...)□

a) processed in a lawful, fair and transparent manner with regard to the data subject (lawfulness,□

loyalty, transparency); b) collected for specified, explicit and legitimate purposes, and not
be further processed in a manner incompatible with those purposes; further processing at
archival purposes in the public interest, for scientific or historical research purposes or for
statistical purposes is not considered, in accordance with Article 89(1), to be incompatible
with the initial purposes (limitation of purposes);

Article 6.1 GDPR

1. Processing is only lawful if and insofar as at least one of the following conditions is
filled:

a) the data subject has consented to the processing of his or her personal data for one or
several specific purposes;

Decision on the merits 34/2020 - 5/35

b) the processing is necessary for the performance of a contract to which the data subject is party or
the execution of pre-contractual measures taken at the latter's request;

c) processing is necessary for compliance with a legal obligation to which the data controller
treatment is submitted;

d) processing is necessary to protect the vital interests of the data subject or of a
other natural person;

e) the processing is necessary for the performance of a task carried out in the public interest or relating to the exercise of
the public authority vested in the controller;

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller
processing or by a third party, unless the interests or fundamental rights and freedoms prevail
of the data subject who require protection of personal data, in particular
when the data subject is a child.

Point (f) of the first paragraph does not apply to processing carried out by public authorities in
the execution of their missions.

GDPR Article 12

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 as well as to carry out any communication under Articles 15 to 22 and of article 34 with regard to the treatment to the data subject in a concise manner, transparent, understandable and easily accessible, in clear and simple terms, in particular for any information intended specifically for a child. Information is provided in writing or by other means including, where appropriate, electronically. When the person concerned so requests, the information may be provided orally, provided that the identity of the data subject is demonstrated by other means.
5. No payment shall be required for providing information under Articles 13 and 14 and for make any communication and take any measure under Articles 15 to 22 and Article 34. When a data subject's requests are manifestly unfounded or excessive, in particular because of their repetitive nature, the controller may: a) require the payment of a reasonable fee which takes into account the administrative costs incurred in providing the information, make communications or take the action requested; or b) refuse to respond to these requests. It is the responsibility of the data controller to demonstrate the character manifestly unfounded or excessive of the request.
6. Without prejudice to Article 11, where the controller has reasonable doubts as to the identity of the natural person submitting the request referred to in Articles 15 to 21, he may request to be provided with additional information necessary to confirm the identity of the concerned person.
- Decision on the merits 34/2020 - 6/35
7. Information to be communicated to data subjects pursuant to Articles 13 and 14 can be provided with standardized icons to provide a good overview, easily visible, understandable and clearly legible, of the intended processing. When the icons are presented electronically, they are machine readable.
8. The Commission is empowered to adopt delegated acts in accordance with Article 92 for the purposes

to determine the information to be presented in the form of icons as well as the procedures governing providing standardized icons.

GDPR Article 13

1. When personal data relating to a data subject is collected

with this person, the data controller provides him, at the time when the data in question

question are obtained, all of the following information:

a) the identity and contact details of the controller and, where applicable, of the representative of the controller;

b) where applicable, the contact details of the data protection officer;

c) the purposes of the processing for which the personal data are intended as well as the basis legal basis for the processing;

d) where the processing is based on Article 6(1)(f), the legitimate interests pursued

by the controller or by a third party; e) recipients or categories of recipients

personal data, if any; and

f) where applicable, the fact that the data controller intends to carry out a transfer of

personal data to a third country or to an international organization, and the existence

or the absence of an adequacy decision issued by the Commission or, in the case of transfers

referred to in Article 46 or 47, or in the second subparagraph of Article 49(1), the reference to guarantees

appropriate or adapted and how to obtain a copy or where to obtain it.

arrangement.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject

data subject, at the time the personal data is obtained, the information

following additional information that is necessary to ensure fair and transparent processing:

a) the retention period of the personal data or, where this is not possible, the

criteria used to determine this duration;

b) the existence of the right to request from the controller access to personal data

personal information, rectification or erasure thereof, or limitation of processing relating to the

data subject, or the right to object to processing and the right to data portability;

c) where the processing is based on Article 6, paragraph 1, point a), or on Article 9, paragraph

2, point a), the existence of the right to withdraw consent at any time, without prejudice to the

lawfulness of processing based on consent given before its withdrawal;

Decision on the merits 34/2020 - 7/35

d) the right to lodge a complaint with a supervisory authority;

(e) information on whether the requirement to provide personal data

personal has a regulatory or contractual nature or if it conditions the conclusion of a contract

and whether the data subject is required to provide the personal data, as well as on the

possible consequences of not providing this data;

f) the existence of automated decision-making, including profiling, referred to in Article 22,

paragraphs 1 and 4, and, at least in such cases, useful information concerning the underlying logic

underlying, as well as the importance and the expected consequences of this processing for the person

concerned.

3. When he intends to carry out further processing of personal data for

a purpose other than that for which the personal data was collected, the

responsible for processing provides the data subject with information in advance about

this other purpose and any other relevant information referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 do not apply where and insofar as the data subject

already have this information.

GDPR Article 14

1. When the personal data was not collected from the person

concerned, the controller shall provide the latter with all of the following information:

a) the identity and contact details of the controller and, where applicable, of the representative of the

controller;

b) where applicable, the contact details of the data protection officer;□

c) the purposes of the processing for which the personal data are intended as well as the basis□

legal basis for the processing;□

d) the categories of personal data concerned;□

e) where applicable, the recipients or categories of recipients of the personal data□

staff ;□

f) where applicable, the fact that the data controller intends to carry out a transfer of□

personal data to a recipient in a third country or an international organization,□

and the existence or absence of an adequacy decision issued by the Commission or, in the case of□

transfers referred to in Article 46 or 47, or in the second subparagraph of Article 49(1), the reference to□

appropriate or suitable warranties and the means of obtaining a copy thereof or the place where they were□

made available.□

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject□

data subject the following information necessary to ensure fair and transparent processing□

with regard to the data subject:□

Decision on the merits 34/2020 - 8/35□

a) the period for which the personal data will be stored or, where this is not□

not possible, the criteria used to determine this duration;□

b) where the processing is based on Article 6(1)(f), the legitimate interests pursued□

by the controller or by a third party;□

c) the existence of the right to request from the controller access to personal data□

personal information, rectification or erasure thereof, or limitation of processing relating to the□

data subject, as well as the right to object to processing and the right to data portability.□

data;□

d) where the processing is based on Article 6, paragraph 1, point a), or on Article 9, paragraph□

2, point a), the existence of the right to withdraw consent at any time, without prejudice to the□

lawfulness of processing based on consent given before its withdrawal;□

e) the right to lodge a complaint with a supervisory authority;□

f) the source from which the personal data originated and, where appropriate, a statement□

indicating whether or not they are from publicly available sources;□

g) the existence of automated decision-making, including profiling, referred to in Article 22,□

paragraphs 1 and 4, and, at least in such cases, useful information concerning the underlying logic□

underlying, as well as the importance and the expected consequences of this processing for the person□

concerned.□

3. The controller shall provide the information referred to in paragraphs 1 and 2:□

(a) within a reasonable period of time after obtaining the personal data, but no later than□

not a month, having regard to the particular circumstances in which the personal data□

personnel are processed;□

b) whether the personal data is to be used for the purposes of communication with the□

data subject, at the latest at the time of the first communication to said person; Where□

(c) if it is intended to communicate the information to another recipient, at the latest when the□

personal data is communicated for the first time. (...)□

GDPR Article 24□

1. Taking into account the nature, scope, context and purposes of the processing as well as the□

risks, of varying likelihood and severity, to the rights and freedoms of individuals□

physical, the controller implements technical and organizational measures□

appropriate to ensure and be able to demonstrate that the processing is carried out□

in accordance with this regulation. These measures are reviewed and updated if necessary.□

2. Where proportionate in relation to the processing activities, the measures referred to in□

paragraph 1 include the implementation of appropriate policies for the protection of□

given by the controller. 3. Application of an approved code of conduct such as the□

Decision on the merits 34/2020 - 9/35□

provided for in section 40 or approved certification mechanisms as provided for in section 42 may

serve as an element to demonstrate compliance with the obligations incumbent on the controller.

GDPR Article 31

The data controller and the processor as well as, where applicable, their representatives

cooperate with the supervisory authority, at the request of the latter, in the performance of its tasks.

Article 66, § 2 of the ACL

The people who are subject to control must lend their assistance.

Article 33 GDPR

1. In the event of a personal data breach, the controller shall notify the

violation in question to the competent supervisory authority in accordance with Article 55, in the

as soon as possible and, if possible, 72 hours at the latest after becoming aware of it, unless

the violation in question is not likely to create a risk for the rights and freedoms of

physical persons. When the notification to the supervisory authority does not take place within 72 hours,

it is accompanied by the reasons for the delay.

2. The processor shall notify the controller of any data breach

staff as soon as possible after becoming aware of it.

3. The notification referred to in paragraph 1 must, at the very least:

a) describe the nature of the personal data breach including, if possible, the

categories and the approximate number of persons concerned by the violation and the categories and the

approximate number of personal data records concerned;

b) the name and contact details of the data protection officer or other contact point

from whom further information may be obtained;

c) describe the likely consequences of the personal data breach;

d) describe the measures taken or that the controller proposes to take to remedy

the breach of personal data, including, where applicable, measures to

mitigate any negative consequences.

4. If and to the extent that it is not possible to provide all information at the same time,□

information may be released in a staggered manner without further undue delay.□

5. The data controller shall document any personal data breach, in□

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

taken to remedy it. The documentation thus compiled enables the supervisory authority to verify□

compliance with the notification obligation.□

Decision on the merits 34/2020 - 10/35□

GDPR Article 37□

1. The controller and the processor shall in any event appoint a data protection officer.□

data protection when:□

a) the processing is carried out by a public authority or a public body, with the exception of□

courts acting in the exercise of their judicial function;□

(b) the core activities of the controller or processor consist of operations□

of processing which, due to their nature, their scope and/or their purposes, require regular monitoring□

and systematic large-scale data subjects; Where□

(c) the core activities of the controller or processor consist of processing□

on a large scale of special categories of data referred to in Article 9 and personal data□

personnel relating to criminal convictions and offenses referred to in Article 10.□

2. A group of companies may appoint a single data protection officer provided□

that a data protection officer is easily reachable from each location□

of establishment.□

3. When the controller or the processor is a public authority or a body□

public, a single data protection officer may be appointed for several authorities or□

organizations of this type, taking into account their organizational structure and size.□

4. In cases other than those referred to in paragraph 1, the controller or processor□

or associations and other bodies representing categories of controllers□

or processors may appoint or, where Union law or the law of a Member State so requires, are required to appoint a data protection officer. The data protection officer can act for these associations and other bodies representing data controllers or subcontractors.

5. The data protection officer is appointed on the basis of his professional qualities and, in particular, its specialist knowledge of the law and practices relating to the protection data, and its ability to carry out the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the data controller, processor or subcontractor, or carry out its tasks on the basis of a service contract.

7. The controller or processor publishes the contact details of the data protection officer data and communicate them to the supervisory authority.

Article 38 GDPR

1. The controller and the processor shall ensure that the data protection officer data is involved, in an appropriate and timely manner, in all questions relating to the protection of personal data.

Decision on the merits 34/2020 - 11/35

2. The controller and the processor assist the data protection officer in carry out the tasks referred to in Article 39 by providing the resources necessary to carry out these missions, as well as access to personal data and processing operations, and to maintain their specialist knowledge.

3. The controller and the processor must ensure that the data protection officer of the data does not receive any instruction with regard to the exercise of the missions. The delegate to data protection cannot be relieved of his duties or penalized by the person responsible for the processing or the subcontractor for the exercise of its missions. The data protection officer reports directly to the highest level of management of the controller or subcontracting.

4. Data subjects may contact the Data Protection Officer at

subject of all questions relating to the processing of their personal data and to

the exercise of the rights conferred on them by this Regulation.

5. The data protection officer is subject to professional secrecy or an obligation to

confidentiality with regard to the exercise of its tasks, in accordance with Union law or

law of the Member States. The data protection officer may carry out other tasks and

tasks. The controller or processor shall ensure that these assignments and tasks

do not involve a conflict of interest.

3. Motivation

3.1.1. With regard to the findings on purpose limitation (Article 5.1

b) GDPR) and the lawfulness of the processing (Article 6.1 GDPR)

12. In essence, the Inspection Service notes in its report² that according to the documents of the

file, the defendant had been aware since 2017 of the fact that Informex SA ensured that

insurance companies may use certain personal data from

of the Crossroads Bank for Vehicles so that, on the basis of this data, these companies

can establish a personalized price offer for potential policyholders.

13. In this regard, the Inspection Service draws attention to the fact that Article 5 of the law of

19 May 2010 establishing the Crossroads Bank for Vehicles (hereinafter the "BCV Law")

lists a limited number of public interest purposes for personal data

included in this Crossroads Bank and on the fact that the personal data

obtained via the Crossroads Bank cannot be used for other purposes.

The Inspection Service claims that confirmation of this can be found in Article 25

² As a reaction to a serious indication from the Management Committee.

Decision on the merits 34/2020 - 12/35

of the Royal Decree of 8 July 2013 implementing the law of 19 May 2010 establishing

of the Crossroads Bank for Vehicles (hereinafter the "AR BCV") which prohibits that data to be

personal data obtained via the Crossroads Bank for Vehicles are used for

'direct marketing' purposes.

3.1.2. The situation before May 25, 2018: the opinion of the CPP of May 11, 2017

14. In its submissions in response, the Respondent states with respect to the first

accusation by the Inspection Service that it had indeed been aware since 2016 of the intention

of Informex SA to be able to identify vehicles on the basis of the license plate

via new activities, namely what are called IRES activities. The defendant explains

that within the framework of these activities, Informex SA wished to offer a service to

insurance companies which would obtain technical data of the vehicle on the basis

of the license plate in order to allow them to immediately establish online a

accurate calculation of the price of car insurance.

15. The documents in the file reveal that this practice consists concretely in

insurers, customers of Informex SA, offer potential policyholders

request a personalized price offer via an online form giving the choice to

persons concerned to manually enter the data of their vehicle or

communicate their license plate, on the basis of which the insurer concerned

then retrieves via Informex SA the vehicle data of the data subject taken over

in the Crossroads Bank. This practice makes it possible in particular to exclude any underinsurance

or overinsurance.

16. The defendant points out that in this context, Informex SA had asked him for access to the

Crossroads Bank for Vehicles, but that he had refused this request because he believed that the

envisaged activities were not part of the purposes of public interest listed in Article

4, 4° of the BCV AR including Informex SA, as an information platform concerning

damaged vehicles³, is charged, namely:

"- (...) safety and (...) better consumer protection (for example

by providing services relating to the assessment of damage caused to

vehicles following an accident, compiling statistics□

on vehicle accidents, communication of information on□

3 See www.informex.be.□

Decision on the merits 34/2020 - 13/35□

vehicles after an accident to the administration, to fight against□

vehicle insurance fraud and safety protection□

vehicles);□

- (...) the overall management of the vehicle fleet, including vehicles not□

of use (for example by providing services in the field of evaluation□

damage caused to vehicles as a result of an accident,□

methods of public sale of vehicles subject to expertise,□

compiling statistics on vehicle accidents and□

communication of information on vehicles after an accident at□

management);□

- (...) allow the technical inspection of vehicles after an accident (for□

example by providing damage assessment services□

caused to vehicles as a result of an accident, and communication□

information on vehicles after an accident to the administration);□

- (...) [the] control by the competent authorities of the regulations relating to□

the management of vehicles put out of use following an accident;□

- (...) the prevention of vehicle insurance fraud."□

17. The defendant therefore considered that in this matter, Informex SA could not invoke□

the exemption from authorization by the Sectoral Committee provided for in article 5 of the BCV AR, pursuant to□

of which: "The natural and legal persons listed in Article 4 (...) are also□

exempted from the prior authorization of the Sectoral Committee with regard to the data□

required□

from□

purposes listed in article 4".□

realization□

for□

the□

18. The Respondent states that he therefore referred Informex SA to the competent Sectoral Committee□

instituted with the Commission for the Protection of Privacy (hereinafter "CPVP") in order to□

to obtain an authorization in accordance with article 18 of the AR BCV.□

19. It appears from the documents in the file that following this, Informex SA had various contacts with the□

OPC, which finally confirmed to him in an opinion of May 11, 2017 that the IRES activities□

fell under the exemption provided for in article 4 of the BCV law juncto article 5 of the BCV RD.□

The CPP states that, although these activities do not specifically concern□

damaged vehicles, they nevertheless result from a preventive use of the□

claims platform of Informex SA and can therefore satisfy the purposes mentioned in□

Article 4 of AR BCV.□

Decision on the merits 34/2020 - 14/35□

20. The CPP has nevertheless restricted the use of these data within the framework of the activities□

mentioned above of several conditions, namely:□

1. Obtaining the license plate of the vehicle of the person concerned by the□

customers of Informex SA can only take place on the basis of the consent of the person□

concerned.□

2. Informex SA must enter into a contract with its customers whereby the latter guarantee□

that the purposes of the processing mentioned in the AR BCV will be respected.□

3. Informex SA must ensure that the persons concerned are previously□

informed of the use made of their license plate.□

4. Informex SA must keep access logs and ensure proper use□

of his service.□

5. Contracts with customers of Informex SA must provide ad hoc mentions concerning□
the use of the license plate as a data identification key□
vehicle technology.□

6. Informex SA and its customers must comply with the provisions of the law (in force at□
the time) of 8 December 1992 relating to the protection of privacy with regard to□
processing of personal data (hereinafter the "LVP"), in particular with regard to□
concerns retention periods and security of processing.□

21. The Respondent draws attention to the fact that on the basis of this opinion of the CPP, he then□
granted Informex SA access to data from the Crossroads Bank for Vehicles.□

22. He adds, however, that before granting access, he checked that the conditions imposed by the□
OPC were respected by Informex SA.□

23. The Litigation Chamber underlines in relation to the above that the opinion issued by the CPVP□
date before the application of the GDPR and that the CPP and its sectoral committees were□
repealed by the law of July 30, 2018 on the protection of individuals with regard to□
processing of personal data (hereinafter "the Framework Law")4. The treatment of□
personal data in question in the context of the IRES activities of Informex SA□
must therefore be confronted since May 25, 2018 with the new legal framework, namely the□
GDPR provisions. The GDPR assumes the responsibility of a person responsible for the□
treatment and does not require the prior consultation and consent of an organization□
external body vested with public authority5.□

4 See article 280 of the law of 30 July 2018 on the protection of natural persons with regard to the processing of□
personal data.□

5 With the exception of Article 36 of the GDPR, not relevant here.□

Decision on the merits 34/2020 - 15/35□

3.1.3. The situation after May 25: confrontation with the GDPR□

A. Identification of the data controllers concerned (Article 4.7 of the GDPR)□

24. In accordance with Article 4.7) of the GDPR, the person responsible for the□
processing: the "natural or legal person, public authority, agency or other□
body which, alone or jointly with others, determines the purposes and means of the□
processing."□

25. The Court of Justice has on several occasions interpreted the concept of "controller"□
broadly in its case law in order to ensure effective and comprehensive protection of□
persons concerned. The Court further underlined that this concept "does not refer□
necessarily to a single organization and may concern several actors participating in this□
processing, each of them being then subject to the applicable provisions in terms of□
data protection"6.□

26. In accordance with Opinion 1/2010 of Group 29, the Litigation Chamber concretely assesses□
the role and quality of the controller(s) concerned7.□

27. In this case, the Litigation Division finds that, for the processing of data to□
personal character obtained via the Crossroads Bank for Vehicles as part of the activities□
IRES, both the defendant and Informex SA and its customers (the insurance companies) must□
be qualified as data controllers, since each defines the purpose and the means□
of its respective treatment processes.□

28. On the Respondent's part, this role of data controller□
concerned stems from article 6 of the BCV law juncto article 30 of the BCV AR, which□
provide that as manager of the Crossroads Bank for Vehicles, he is the□
responsible for the processing of personal data contained in this□
Crossroads bank.□

29. With regard to Informex SA, article 5 of the BCV Law juncto article 4, 4° of the BCV AR□
stipulates that this company processes the personal data included in the□

6 See in particular CJEU, 5 June 2018, C-210/16 - Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388, recitals□

27-29.□

7 See Group 29, Opinion 1/2010 on the notions of "controller" and "processor", 16 February 2010 (WP 169),□

as specified by the DPA in a note "Update on the notions of controller / processor with regard to□

of Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal da□

personnel (GDPR) and some applications specific to liberal professions such as lawyers".□

Decision on the merits 34/2020 - 16/35□

Crossroads bank for vehicles in the context of the fulfillment of the purposes of interest□

listed in Article 5 of the BCV Law for which it is responsible (see point 16 above).□

30. Apart from the defendant and Informex SA, the customers of the latter, namely the companies□

insurance companies, must also be qualified as data controllers within the meaning of□

Article 4(7) of the GDPR for the processing processes they carry out, namely the□

processing of personal data in the context of establishing their offers□

personalized prices.□

31. Each of the aforementioned parties is therefore, in its capacity as controller,□

in accordance with the responsibility provided for in Articles 5.2 and 24 of the GDPR, obliged to respect□

the principles of the GDPR for its processing process and must be able to□

to prove.□

B. Lawful bases for processing (Article 6.1 of the GDPR)□

32. In accordance with Article 6.1 of the GDPR, processing of personal data is only□

lawful only if, and insofar as, it is based on one of the bases of lawfulness listed□

in this article.□

33. The processing of personal data included in the Crossroads Bank for□

vehicles is carried out by each of the processing managers identified above on a□

different basis of lawfulness.□

34. However, the question arises as to whether these bases of lawfulness can be used for the□

processing at issue in this proceeding, or in the context of IRES activities□

of Informex SA, data obtained via the Crossroads Bank for Vehicles is transmitted

to third parties (i.e. insurers who are customers of Informex SA).

35. The defendant processes the data of the Crossroads Bank for Vehicles on the basis of Article 6

of the BCV Law juncto article 30 of the RD BCV, which provide that the defendant is responsible

the processing of personal data contained in the Crossroads Bank for

vehicles. In this capacity, the respondent is therefore responsible for the treatment of these

data and under the responsibility provided for in Articles 5.2 and 24 of the GDPR, it is required to

ensure that it is processed in accordance with the Processing Principles

of personal data of article 5.1 of the GDPR.

Decision on the merits 34/2020 - 17/35

36. For the processing of personal data obtained via BCV, Informex SA uses

as the basis for the processing, the missions of public interest conferred on it by the RD BCV

(see point 16 above).

37. It appears from the documents in the file that Informex SA more precisely bases the transmission of

data from the Crossroads Bank for Vehicles to insurers as part of IRES activities

- with a view to establishing personalized price offers for insurance - on the purposes

interest listed in Article 4, 4°, points 1 and 5 of AR BCV, namely: "the security and

better consumer protection (...)" and "the prevention of insurance fraud

vehicle”⁸.

38. Customers of Informex SA - insurers - process personal data

in accordance with Article 6.1 a) of the GDPR on the basis of the consent of the persons

concerned.

39. The documents in the file show more precisely that, in the context of IRES activities, the

customers of Informex SA offer potential policyholders who request an offer of

online price for vehicle insurance, the possibility of communicating their license plate

registration number, which is then used as an identification key by Informex customers

SA to retrieve vehicle data from the Vehicle Crossroads Bank.□

40. In this context, the consent of the persons concerned is requested via a□

pop-up notification in which you must answer the question "Do you accept that we□

use your plate number to be able to make you an offer?" with "I accept" or□

"I refuse".□

41. With regard to this basis of lawfulness, the Litigation Chamber draws attention to the fact□

that the consent is only valid if it meets the conditions set out in article 4.11 and in□

recital 32 of the GDPR⁹ and if it concerns processing that is not prohibited by law□

(see point C.2 below).□

8 Exhibit 7 to the Respondent's Record.□

9 Article 4.11) of the GDPR defines a valid consent as being: "any expression of will, free, specific,□

informed and unambiguous by which the person concerned accepts, by a declaration or by a clear positive act, that□

personal data relating to him or her are processed". Recital 32 of the GDPR specifies that a□

consent "must [...] be given by a clear positive act by which the data subject manifests freely,□

specific, informed and unequivocal consent to the processing of personal data concerning him, for example at the□

means of a written statement, including by electronic means, or an oral statement. This could be done in particular□

by ticking a box when consulting a website, by opting for certain technical parameters for services□

of the information society or by means of another statement or other conduct which clearly indicates in this□

context that the data subject consents to the proposed processing of his or her personal data."□

Decision on the merits 34/2020 - 18/35□

C. Purpose limitation (Article 5.1.b) of the GDPR)□

C.1. General□

42. In accordance with Article 5.1 b) of the GDPR, personal data must be□

"collected for specified, explicit and legitimate purposes, and not to be processed□

subsequently in a manner incompatible with those purposes; further processing for the purposes□

archives in the public interest, for scientific or historical research purposes or for□

statistical purposes shall not be considered, in accordance with Article 89(1), as

incompatible with the initial purposes"; This article thus describes one of the basic principles relating to the processing of personal data, i.e. the so-called "limitation of purposes".

43. With regard to the processing of personal data included in the Bank-crossroads of vehicles, it is appropriate, in the light of this provision of the GDPR, to refer to article 5 of the BCV Law juncto article 4 of the RD BCV, which contain an exhaustive list of legal persons who have access to the Crossroads Bank for vehicles and purposes for which these legal persons may process the aforementioned data (see above).

44. It is on the basis of these legal provisions (and more specifically of article 4, 4° of AR BCV) that as data controller, Informex SA also processes data from the Bank-crossroads of vehicles for the realization of the skills and purposes which it are conferred by the AR.

45. As already indicated above, as an information platform for vehicles victims, Informex SA bases the processing in question more precisely on the purposes of interest public referred to in Article 4, 4°, points 1 and 5 of AR BCV, namely: "safety and better consumer protection (...)" and "the prevention of vehicle insurance fraud".

46. The Litigation Chamber is however of the opinion that the service offered by insurers, allowing, on the basis of the license plate, to consult the data of the vehicle in the Banque-crossroads for vehicles in order to establish personalized price offers, can be classified in these public interest purposes of AR BCV. This service concerns the commercial relationship between the insurer and its customers and not the performance by Informex SA of missions conferred on it by this RD aiming (among other things) at protecting consumers and fraud prevention.

Decision on the merits 34/2020 - 19/35

47. The Litigation Division therefore considers that this processing violates the principle of

limitation of purposes contained in Article 5.1 b) of the GDPR.□

C.2. "Direct Marketing Purposes"□

48. Secondly, it should be noted that in accordance with Article 25 of the AR BCV,□

"Personal data obtained via the Crossroads Bank cannot be□

used for 'direct marketing' purposes".□

49. The question therefore arises whether, in this case, the treatment of the plate□

of registration by Informex SA customers, and more specifically the use of this□

personal data as an identification key for the establishment of price offers□

personalized for potential policyholders (data subjects), must be□

considered as "direct marketing" within the meaning of article 25 of AR BCV.□

50. Although the BCV RD contains an explicit ban on the use of data contained□

in the Crossroads Bank for direct marketing purposes, the RA itself does not give any□

definition of this concept.□

51. In the RA Report to the King, this prohibition is explained as follows: "Because the□

private associations, and not only public services and non-profit organizations offering□

sufficient guarantees of independence from the commercial sector and the application of the□

LVP must also be able to consult certain data via the Crossroads Bank,□

it is explicitly specified that the personal data obtained via the□

Banque-Carrefour cannot be used for 'direct marketing' purposes.□

52. The GDPR also uses the notion of "direct marketing"□

in its article 21 concerning the right of opposition, but does not contain either a definition□

of this concept.□

53. It is for this reason in particular that the Data Protection Authority has drawn up the□

January 17, 2020 its Recommendation No. 01/2020 in which, developing the definition□

included in the proposal for a Regulation of the European Parliament and of the Council on the□

respect for privacy and the protection of personal data in the□

electronic communications and repealing Directive 2002/58/CE, it defines the notion of

"direct marketing" as follows:

10 COM(2017) 10. Article 4 of the proposal defines: "direct marketing communications": any form

advertising, both written and oral, sent to one or more end users, identified or identifiable, of services of

Decision on the merits 34/2020 - 20/35

"Any communication in any form, whether solicited or unsolicited, from

of an organization or a person and aimed at the promotion or sale of services,

products (paid or not), as well as brands or ideas, addressed by an organization

or a person acting in a commercial or non-commercial context, which is addressed

directly to one or more natural persons in a private or professional context and

involving the processing of personal data."¹¹

54. It follows first of all from this definition that not only communications not

solicited but also solicited communications should be considered as

direct marketing if and insofar as they are aimed at the promotion and/or sale of goods or

of services, are directly addressed to one or more natural persons and involve

the processing of personal data.

55. Recommendation No. 01/2020 specifies in this respect that "communications addressed to a

prospect, to an interested person or to a customer/affiliate/subscriber/member, are just as much

direct marketing communications" and that a prospect or an interested person

distinguishes from a customer in that it is a potential customer who has requested information

on the products or services of the organization concerned but which has not yet concluded any

engagement with it.

56. In view of the foregoing, the Litigation Chamber considers that the practice in question

whereby the customers of Informex SA - who are automobile insurers and therefore act on

privately - process personal data obtained via the Crossroads Bank for

vehicles"¹² in order to establish a personalized price offer must indeed be considered

as direct marketing and therefore falls under the prohibition of article 25 of the AR BCV.□

57. The processing of personal data by the Crossroads Bank in question concerns□

especially :□

i.□

ii.□

“a solicited or unsolicited communication”, in this case the communication□

a personalized price offer to potential policyholders;□

“emanating from an organization acting in a commercial context”, namely the□

insurance company, client of Informex SA;□

electronic communications, including by means of automated communication and calling systems, with or without□

human intervention, by e-mail, by SMS, etc.”.□

11 Recommendation of the Data Protection Authority n° 01/2020 of January 17, 2020 relating to data processing□

of a personal nature for direct marketing purposes, point 14.□

12 See article 25 of AR BCV.□

Decision on the merits 34/2020 - 21/35□

iii.□

iv.□

v.□

“aimed at (...) the sale of services, products”, in this case the sale of a□

car insurance ;□

“which is addressed directly to one or more natural persons”, namely the□

data subjects who are requesting a quote for insurance;□

and□

“involving the processing of personal data”, in this case the plate□

registration as an identification key to extract data from the□

Banque-crossroads for vehicles, as well as personal identification data□

concerned.□

58. The Litigation Chamber considers that the fact that the processing of the data in question by□
customers of Informex SA takes place on the basis of the consent of the persons concerned□
does not mean that this processing is valid in this case, since the use of the data□
personal data in question for this processing purpose - namely marketing□
direct - is absolutely and explicitly prohibited by law (article 25 of the RD BCV).□
Consent can never be valid if it relates to processing that is□
illegal.□

59. In addition, this practice requires the processing of personal data by various□
players, including also Informex SA which - at the request of its customers and on the basis of□
license plate number as identification key - extracts data□
necessary from the Banque-crossroads for vehicles. In this case, Informex SA processes this data□
with the aim of allowing its customers to establish a personalized price offer for a□
car insurance. As mentioned above, the aforementioned purpose does not appear in the□
exhaustive list of the purposes of article 4, 4° of the AR BCV, with the consequence that such□
processing constitutes a breach of the purpose limitation principle of Article 5.1 b) of the□
GDPR for Informex SA.□

3.1.4. Conclusion□

60. With regard to the findings of the Inspection Service regarding the lawfulness of the□
processing and limitation of purposes, the Litigation Chamber emphasizes that processing□
does not take place in a lawful manner when the basis of lawfulness on which an official of the□
processing processes certain personal data is used for the processing of□
this personal data for purposes other than those determined by□
limited manner by the lawfulness basis applied.□

Decision on the merits 34/2020 - 22/35□

61. In this case, the Litigation Chamber considers that the processing by which data to be□

personal nature of the Crossroads Bank for Vehicles are transmitted by Informex SA to its customers in order to enable them to establish personalized price offers cannot appear in the number of the purposes of public interest of article 4 of the RD BCV and that consequently, it constitutes a violation of Articles 5.1 b) (purpose limitation principle) and 6.1 of the GDPR (lawfulness of processing). This processing concerns the commercial relationship between the insurers and their (potential) customers and is not necessary for the performance of the tasks of public interest granted to Informex SA by AR BCV.

62. The Litigation Chamber also draws attention to the fact that under Article 25 of AR BCV, data obtained via the Crossroads Bank for Vehicles cannot be processed for direct marketing purposes. The practice in question whereby customers of Informex SA - which are car insurers and therefore act in a private capacity - process personal data obtained via the Crossroads Bank for Vehicles¹³ with a view to establish a personalized price offer must indeed be considered as marketing direct and therefore falls under the prohibition of article 25 of the AR BCV.

63. The Litigation Chamber specifies that the GDPR does not prevent the processing in question by insurance companies on the basis of the consent of the persons concerned as such, subject to the conditions set out in the GDPR, but that this Framework - namely AR BCV - does not authorize this processing. However, if the legislator considers that this practice serves the public interest, the legal regulation should be adapted in this sense. In this regard, the Litigation Division grants the defendant a longer period longer than usual (i.e. six months) to bring the processing into compliance.

64. The Litigation Chamber points out that in its capacity as manager of the Crossroads Bank for vehicles and responsible for the processing of personal data therein, on occasions, the defendant must ensure that they are treated according to the principles of the processing of personal data and in accordance with the legal framework in force.

65. The Litigation Chamber notes however, on the basis of the documents in the file, that in

the case, the defendant acted in good faith and in accordance with the opinion of the former OPC, and

that in its capacity as controller, it has also ensured compliance with this notice.

The Litigation Division therefore considers that¹⁴, under the principle of legal certainty,

the trust established by the opinion of the CPP cannot be betrayed and that therefore the

¹³ See article 25 of AR BCV.

¹⁴ A. MAST, J. DUJARDIN, M. VAN DAMME, J. VANDE LANOTTE, *Overzicht van het Belgisch administratief recht*, Mechelen,

Wolters Kluwer, 2014, 53-54.

Decision on the merits 34/2020 - 23/35

Respondent cannot be penalized for past breach of limitation principle

purposes under Article 5.1 b) of the GDPR and the requirement of lawfulness of processing

prescribed by Article 6.1 of the GDPR.

66. The Litigation Chamber therefore considers that a violation of Articles 5.1 b) and

6.1 of the GDPR can be observed but that - given the principle of legal certainty and the

trust established by the opinion of the CPVP of May 11, 2017 on the part of the defendant -, no

sanction cannot be imposed on the latter.

3.1.5. The deliberations of the information security committee

67. Following the findings of the Inspection Service, in this case concerning the lawfulness of the processing

and purpose limitation, the defendant submitted to the Data Protection Authority

several deliberations of the Information Security Committee (hereinafter 15 "CSI") with a view to

confront higher legal standards. By this request, the defendant seeks to obtain

legal certainty and whether the communication of personal data

authorized by these deliberations is GDPR compliant. The defendant also requested

in this respect to the Data Protection Authority to confirm, despite these deliberations of the

CSI authorizing the transmission of personal data, if in its capacity as

controller, he can still decide not to transmit these

data.

68. The above deliberations are particularly important for the present case.□

given that through them, the CSI authorizes the communication of data from the Bank-□

crossroads of vehicles - namely the license plate number - to those responsible□

processing who request them for processing purposes with a commercial aspect.□

This despite the defendant's reasoned position on the matter, which considered in both cases□

that such processing would not comply with the principles of the GDPR. In the first case 17, the□

respondent stated more specifically that there were no valid grounds for admissibility since□

the processing of the license plate number was not necessary to respond to□

a legal obligation incumbent on the controller or to perform a task□

of general interest incumbent on this same data controller. In the second case, the□

defendant believed that the processing of the license plate number was not□

15 Exhibits 32A and 32B of the defendant's file.□

16 Deliberation No. 19/027 of September 3, 2019, amended on January 14, 2020 and Deliberation No. 20/005 of February 4, 20□

two of the federal authority chamber of the CSI.□

17 Deliberation No. 19/027, point 5.□

Decision on the merits 34/2020 - 24/35□

in accordance with the data minimization principle of Article 5.1 c) of the GDPR, since the□

intended purpose could be achieved by processing the chassis number.18 19□

69. In other words, the content of these deliberations of the CSI may create for the defendant□

expectations that are contrary to the position that the latter - in his capacity as head of the□

processing of the personal data concerned and under the principle of□

liability set out in the GDPR - had originally adopted regarding communications□

personal data in question.□

70. Within the current legal framework, and more specifically under article 35/1 of the law of 15 August□

2012 relating to the creation and organization of a federal service integrator and the law of□

September 5, 2018 establishing the information security committee, the CSI is notably□

competent to issue deliberations concerning certain data communications□

of a personal nature, including also the communication of data included in the Bank-□

crossroads of vehicles.20□

71. Article 35/1, § 4 of the Federal Services Integrator Act specifies that "The deliberations of the□

information security committee are reasoned and have a binding general scope□

between the parties and towards third parties."21□

72. In the preparatory works of the law of 5 September 2018, it is stated that "it is essential□

to be able to issue binding general decisions in the form of□

deliberations. This offers all actors legal certainty as to the fact that a sharing of□

data is legally permissible as long as they properly comply with the□

conditions provided for in the deliberation."22.□

73. The Litigation Division understands the importance of obtaining legal certainty through□

actors prior to the processing of personal data. However, she considers□

that the promulgation of binding decisions concerning the processing of personal data□

personal character is contrary to the philosophy and provisions of the GDPR. This is□

particularly important since these decisions have direct consequences for the rights□

of third parties to the protection of their personal data.□

18 Deliberation No. 20/005, point 6.□

19 The Chambre du Conseil points out that in the context of this case where Informex SA transmits data of a□

staff of the Crossroads Bank for Vehicles to insurance companies, no deliberation was issued by the CSI.□

20 Law of 15 August 2012 relating to the creation and organization of a federal service integrator;□

21 [proper underlining].□

22 See Doc. Speak. Chamber, 2017-2018, no. 3185/001, p. 6; [proper underlining].□

Decision on the merits 34/2020 - 25/35□

74. The Litigation Division draws attention in particular to the liability introduced by the□

GDPR, included in article 5.2 juncto article 24 of the GDPR, which constitutes one of the central pillars□

of the GDPR and under which controllers must be able to demonstrate

that it processes personal data in accordance with the principles relating to the

processing of personal data listed in article 5.1 of the GDPR.

75. The Litigation Chamber emphasizes that such a system therefore creates a situation

ambiguous for data controllers, such as the defendant in this case, who is expected to

that it gives access to the personal data concerned by the deliberations issued

by the CSI on the one hand²³, but which is required, by virtue of the principle of responsibility, to act

even proactively to ensure that the principles relating to data processing

of a personal nature have been respected and to be able to demonstrate it, on the other hand. This implies

a risk of disempowerment of data controllers, which is incompatible

with the principles of the GDPR and contrary to articles 5.2 juncto 24 of the GDPR. 24

76. It is not for the Litigation Chamber to question the role of the CSI - this

rests with the legislator - nor the relevance of the analyzes of such a body in practice.

However, the Litigation Chamber notes that in themselves, the deliberations of the CSI cannot

form a basis for treatment. Of course, under the current legal framework, these

deliberations have significant significance given the fact that those responsible for the

processing may invoke the principle of trust.

77. The Litigation Chamber emphasizes in this regard that the issuing of a deliberation by the CSI does not

can ever imply an obligation for the data controller concerned to

communicate personal data. The latter retains full freedom

to appreciate the opportunity himself.^{25 26}

²⁵ Opinion No. 34/2018 of 11 April 2018 of the Commission for the Protection of Privacy (CPVP) concerning a preliminary draft

law establishing the information security committee and amending various laws concerning the implementation of the Regulation

2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of individuals with regard to

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

(CO-A-2018-017), paragraph 13.

25 Opinion No. 34/2018 of 11 April 2018 of the Commission for the Protection of Privacy (CPVP) concerning a preliminary draft law establishing the information security committee and amending various laws concerning the implementation of the Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (CO-A-2018-017), item 13.

25 Opinion No. 34/2018 of 11 April 2018 of the Commission for the Protection of Privacy (CPVP) concerning a preliminary draft law establishing the information security committee and amending various laws concerning the implementation of the Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (CO-A-2018-017), point 13.

26 Explanatory memorandum to article 18 of the law of 5 September 2018 establishing the information security committee.
Decision on the merits 34/2020 - 26/35

78. The Litigation Chamber also points out that after deliberation by the CSI, all principles of the GDPR remain of course applicable, including the principle of responsibility (articles 5.2 juncto 24 of the GDPR). However, CSI analysis can play an important role in accountability by a controller. Indeed, to assess the whether a controller meets the accountability requirement in a specific case, the Litigation Chamber will start from the assumption that the analysis can be relied upon of a public authority such as the CSI.

With regard to compliance with the liability of the controller (Article 24 of the GDPR), security of processing (Article 32 GDPR) and notification to the supervisory authority a personal data breach (Article 33 of the GDPR)

3.2.

79. In its report, the Inspection Service states that "exhibits 4, 5 and 13 show that [the defendant] refers to the letter from the Privacy Commission of the 11/05/2017 (...) to support its position that (1) the fact that Informex Sa ensures that

that insurance companies may use certain personal data□

from the Crossroads Bank for Vehicles so that these companies can provide□

personalized price offer to data subjects is legitimate and (2) Informex SA must□

take measures to better secure the personal data concerned by□

matter". [Note: The passages quoted from the report of the Inspection□

books made by the General Secretariat of the Authority in the absence of official translations]□

The Inspection Service further notes that the defendant "does not [demonstrate] that [he] took□

appropriate security measures and that it has notified the DPA of a data breach to□

personal character".□

80. With respect to this allegation, the Respondent states in its submissions in response□

that its initial position was that the "IRES activities" of Informex SA did not come under the□

exemption from authorization in accordance with article 4 juncto article 5 of the RD BCV and it underlines□

that it had adapted this position following the opinion of the CPP of May 11, 2017.□

81. The Respondent adds to this that before granting access to the Crossroads Bank for Vehicles, it□

ensured that the conditions imposed by the CPVP were respected by Informex SA□

(see above).²⁷□

²⁷ See above.□

Decision on the merits 34/2020 - 27/35□

82. Finally, the Respondent argues that there can be no question of unauthorized communication of□

data nor of breach of personal data since it could legitimately be□

rely on the aforementioned opinion of the CPP.□

83. The Litigation Chamber finds on the basis of the documents in the file that the defendant acted□

in accordance with the notice issued by the CPVP to Informex SA on May 11, 2017.□

The respondent indeed adds to its submissions in response the correspondence with Informex□

SA in which, in his capacity as controller, he asks the latter to□

provide all information and documentation relating to the treatment of the plate□

of registration within the framework of the IRES activities of Informex SA.□

84. Although the Litigation Division considers that the processing in question involves a violation□
of personal data within the meaning of Article 33 of the GDPR, it repeats in this regard□
that by virtue of the principle of legal certainty, the confidence established by the opinion of the CPP□
cannot be betrayed and therefore the defendant cannot be punished for□
have in the past granted access to the Crossroads Bank for Vehicles to Informex SA in the□
framework of "IRES activities".□

85. The Litigation Chamber therefore considers that a violation of Articles 24, 32 and□
33 of the GDPR can be ascertained but that - given the principle of legal certainty and trust□
established by the opinion of the CPVP of May 11, 2017 on the part of the defendant -, no sanction□
can be inflicted on him.□

3.3.□

With regard to the finding relating to the appointment of the Data Protection Officer□
data (Article 37 GDPR) and its position (Article 38 GDPR)□

86. In its report, the Inspection Service notes that "[the defendant] did not [demonstrate]□
how is the concrete choice of Mr. Y to exercise the function of delegate□
to data protection" and that "[the defendant] did not [provide] copies of documents□
certifying that Mr. Y has been notified to the DPA as delegate for the protection of□
data". Finally, the Inspection Service asserts that "[the defendant] does not demonstrate that in□
As data protection officer, Mr Y is associated, in a way□
appropriately and in a timely manner, to all questions relating to data protection to□
personal character and that he can accomplish his missions in complete independence".□

28 A. MAST, J. DUJARDIN, M. VAN DAMME, J. VANDE LANOTTE, Overzicht van het Belgisch administratief recht, Mechelen,
Wolters Kluwer, 2014, 53-54.□

Decision on the merits 34/2020 - 28/35□

87. With respect to this accusation, the Respondent states in its submissions in response□

that Mr. Y's choice was based on his in-depth knowledge of the organization, his

knowledge of ICT as well as his developed analytical and synthetic thinking.

The defendant also points out that Mr. Y took the "certified Data Protection

Officer" with success and that he thus obtained ISO 27005 ('Risk Manager') and ISO 270010 ('Lead

Implementer'), and attaches proof.²⁹

88. With regard to the registration of Mr. Y as a delegate for the protection of

data with the Data Protection Authority, the defendant declares to have been

informed on September 24, 2019 that obviously due to a technical problem,

something had gone wrong when registering his protection officer

of the data, since the Inspection Service had not been able to find his registration in

the database of the Data Protection Authority. The defendant states that after

having become aware of this fact, he restarted the online check-in and received a

confirmation.

89. The Litigation Chamber draws attention to the fact that under Article 37.1, a) of the GDPR,

the defendant has the obligation - since it is a public authority - to appoint a delegate to

data protection that meets the requirements listed in Articles 37 to 39 of the

GDPR.

90. The Litigation Chamber finds on the basis of the documents communicated that the delegate to the

data protection appointed by the defendant was appointed in accordance with Article 37.5 of the

GDPR, on the basis of his professional qualities and his specialized knowledge of the

data protection law and practices. This is particularly apparent

certificates attached to the pleadings in response concerning the formation of "certified DPO"

and certificates obtained by the interested party.

91. The Litigation Chamber therefore considers that no violation of Articles

37 and 38 GDPR.

3.4.

As regards the findings relating to compliance with the obligation to cooperate (Article

31 of the GDPR and article 66, § 2 of the LCA)

29 Exhibit 23 to the Respondent's Record.

Decision on the merits 34/2020 - 29/35

92. In its report, the Inspection Service notes with regard to compliance by the

defendant of the obligation of cooperation provided for in Articles 31 of the GDPR and 66, § 2 of the

LCA firstly that the latter did not answer the questions asked by the Service

Inspection within the time limit of one month. Secondly, the Inspection Service finds

that the defendant did not provide a copy of the documents justifying the choice of Mr. Y in

as Data Protection Officer.

93. With respect to the first prong of this charge, the Respondent asserts in its

conclusions in response that this non-compliance with the deadline imposed by the Inspection Service was

due to a case of force majeure, namely the death of a member of the employee's family

responsible for answering these questions and the short-term absence of the latter, which

result. The defendant also points out that this was reported by another

employee on July 2, 2019 (i.e. four days before the expiry of the imposed deadline) at

the Data Protection Authority and that it had been announced that therefore the response

would be sent a few days late. The defendant adds in conclusion that the

response was finally provided only three days after the deadline for response had expired.

94. The Litigation Chamber considers that with regard to the first accusation, the case of force

major invoked by the defendant justifies a delay of three days and that this cannot be

considered a violation of the obligation to cooperate within the meaning of Article 31 of the GDPR

in the head of the latter.

95. With regard to the second part of this accusation, it should be emphasized that the

respondent annexed to its pleadings in response a copy of the documents which

support the choice of Mr Y as data protection officer. It's more

precisely the job description for the position as well as the ISO certificates obtained

by the interested party.³⁰

96. The Litigation Chamber therefore considers that no violation of the

articles 31 of the GDPR and 66.2 of the LCA.

As regards the finding relating to compliance with the obligation of transparency (Article

12 of the GDPR) and the information to be provided (Articles 13 and 14 of the GDPR)

3.5.

30 Exhibits 23 and 24 of the defendant's file.

Decision on the merits 34/2020 - 30/35

97. With regard to compliance with the obligation of transparency and the information to be provided in

Pursuant to Article 13 of the GDPR, the Inspection Service notes in its report that several

elements that are required by the GDPR are not included in the privacy statement

of the defendant, namely:

- "the mention of the purposes of the processing for which the personal data

are intended (as formulated in the sentence "The purposes for which we process

your personal data mainly concerns the fulfillment of obligations

legal and the execution of our missions of public interest or relating to the exercise of

public authority") as well as the mention of the legal basis for the processing (according to

the formulation "the legislation in force") [are] formulated in a general and vague manner

so that they are neither transparent nor accessible for the persons concerned;

- the mention of the recipients of the personal data (according to the wording

"State administrative services", "Countries with which Belgium has entered into

conventions or agreements", "[...]" and "Third Parties") is formulated in a general way and

vague, so that without additional information, the list of recipients is not

not

(....)".

[Editor's note: the quoted passages of the defendant's confidentiality statement have been

freely translated by the ODA General Secretariat in the absence of translation

official]

the people

clear for

concerned

;

98. The Respondent states in its submissions in response and during the hearing of May 4, 2020

concerning this accusation that a first correction has already been made during the

procedure, but that the new version of the privacy statement is still in

project. The defendant adds to this that this new version was on the agenda

a meeting of the management committee which could not take place due to the crisis of the

coronavirus and indicates that it is planned for the next few days.

99. The Litigation Chamber draws attention to the fact that in accordance with Article 12.1 of the

GDPR, the controller "[takes] appropriate steps to provide any

information referred to in Articles 13 and 14 as well as to carry out any communication under

of Articles 15 to 22 and Article 34 with regard to the processing to the data subject

in a concise, transparent, comprehensible and easily accessible manner, in terms

clear and simple (...).".

100. Recitals 58 and 60 specify that "The principle of fair and transparent processing requires

that the data subject is informed of the existence of the processing operation and its

purposes" and that "The principle of transparency requires that any information sent to the public

or the data subject is concise, easily accessible and easy to understand (...).".

Decision on the merits 34/2020 - 31/35

101. The Litigation Chamber notes first of all that the declaration of confidentiality of the

defendant is incomplete with regard to the personal data collected and

processed by him. In point 6 of its privacy statement, the respondent states ☐
in fact that it can process "personal data of various kinds" and that it "[can] ☐
include, among other things, identification data (surname, first name, date of birth, etc.), ☐
contact details (address, telephone number, etc.). Further on in point 6 of the declaration of ☐
confidentiality, the following is repeated: "The categories of personal data which ☐
are processed by the FPS Mobility and Transport are more specifically: ☐
• identification data (surname, first name, date of birth, etc.) ☐
• contact details (postal address or e-mail address, telephone number, etc.) ☐
• [...]" ☐

102. If and to the extent that personal data not obtained from ☐
data subjects are processed, Article 14.1, d) of the GDPR provides that the categories ☐
personal data concerned must be specified. In a general view, ☐
a privacy statement cannot contain an ellipsis, as this ☐
emphasizes its imprecise and incomplete character. ☐

103. Secondly, it should be noted that the privacy statement does not mention ☐
not in sufficient detail the basis of lawfulness of Article 6.1 of the GDPR on which the ☐
defendant bases the processing of the personal data collected by him. ☐

104. In this regard, the Litigation Chamber notes, thirdly, that the defendant does not define ☐
nor is it sufficiently precise the purposes of the processing for which the ☐
personal data is collected. In point 6, § 2 of the declaration of ☐
confidentiality, there seems to be confusion between the basis of lawfulness and the purposes ☐
processing and it reads: "The purposes for which we process your data ☐
personal nature mainly concern compliance with legal obligations and the execution ☐
our tasks in the public interest or in the exercise of public authority". ☐

105. The information thus provided to the persons concerned is worded too ☐
succinct and in terms that are too vague and do not allow them to sufficiently ☐

understand the basis of lawfulness and the purposes of the processing.□

106. In accordance with the guidelines on transparency drafted by the Group 29, the□

information provided on the basis of Articles 13 and/or 14 of the GDPR must be concrete and□

final and may not include any abstract or ambivalent formula. The Group 29□

Decision on the merits 34/2020 - 32/35□

specifically states that "Qualifiers such as 'may', 'could', 'some',□

"often" and "possible" are to be avoided" and that "When controllers□

choose to use vague terms, they should be able, in accordance with the principle of□

responsibility, demonstrate that this type of language could not be avoided and prove that it□

does not affect the fairness of the “31 treatment.” The Group 29 emphasizes that this is particularly□

for the purposes of the processing and for its legal basis.□

107. Fourthly, it should be noted that the retention period for the data to be□

personal character is also not sufficiently specified to meet the requirements□

of Article 13.2 and Article 14.2, a) of the GDPR. Point 6, § 3 of the declaration of□

confidentiality only indicates that the personal data concerned□

"are kept for a period not exceeding that necessary for the purposes□

for which they are processed". However, it is apparent from the Group Guidelines 29□

that such a formulation is insufficient. Group 29 stresses in this respect that the deadline /□

mention of the retention period is linked to the principle of data minimization set out in□

Article 5.1, c) of the GDPR as well as the storage limitation requirement set out in Article□

5.1, e) GDPR. It specifies that "The retention period (or the criteria for determining it)□

may be dictated by different factors such as regulatory requirements or lines□

industry guidelines, but it should be worded in such a way that the person□

concerned can assess, depending on the situation in which it finds itself, what will be the period□

conservation in the case of specific data or in the case of specific purposes.”32□

108. Fifthly, the Litigation Chamber finds that the declaration of confidentiality of the□

respondent does not contain an exhaustive list of (categories of) data recipients□

that it has collected, as required by Articles 13.1 and 14.1, e) of the GDPR. In this regard, the point□

9 of the privacy statement states in particular the following:□

"Your data may be communicated to third parties on the basis of our legal obligations□

and regulations but also within the framework of the execution of our missions of public interest or□

subject to the exercise of public authority. (...)□

31 "Guidelines on transparency within the meaning of Regulation (EU) 2016/679", adopted on November 29, 2017 by the□

29, p. 11.□

32 "Guidelines on transparency within the meaning of Regulation (EU) 2016/679", adopted on November 29, 2017 by the□

29, p. 46.□

Decision on the merits 34/2020 - 33/35□

As part of the execution of its legal missions, [the defendant] is sometimes obliged to□

receive or communicate your personal data, more specifically to□

following recipients:□

- yourself□

- other recipients depending on the legal obligations and authorizations for the□

information and the exchange of information, such as:□

- o other FPS services□

- o State administrative services□

- o countries with which Belgium has concluded conventions or agreements□

- o [...]□

- some thirds□

- [...]”□

109. Also on this point, the privacy statement contains conditionals and□

ellipses, which indicate that the persons concerned are not completely□

informed of the possible transfer of their personal data.□

110. The Litigation Chamber stresses the importance of respecting the obligations of transparency□
on the part of a data controller given the impact this has on the exercise of rights□
of the data subjects set out in Articles 15 to 22 of the GDPR, as illustrated in the□
case law of the Court of Justice.³³□

111. The Litigation Chamber further emphasizes that as a public authority, the defendant has□
an exemplary role in terms of compliance with data protection legislation□
of a personal nature and that, in addition, it processes a large quantity of data□
personal character and that therefore, in accordance with the principle of "lead by example",□
he must ensure at all times to act in accordance with this legislation and in particular to□
comply with the aforementioned essential provisions of the GDPR concerning□
the□
transparency.³⁴□

112. The Litigation Division therefore considers, for the reasons set out above, that one must□
find in this case a violation of Articles 12, 13 and 14 of the GDPR.□

33 Court of Justice, 1 October 2015, Bara, C-201/14.□

34 Data Protection Authority, Strategic Plan 2020-2025",□

https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/APD_Plan_Strategique_28012020.pdf, p.□
25.□

Decision on the merits 34/2020 - 34/35□

3.6.□

Publication of the decision□

113. Given the importance of transparency regarding the decision-making process of the Chamber□
Litigation, in accordance with Article 95, § 1, 8° of the LCA, this decision is published□
on the website of the Data Protection Authority, mentioning the data□
of identification of the defendant³⁵, and this because of the specificity of the present decision - this□
which makes re-identification inevitable, even in the event of deletion of the data□

of identification - as well as the public interest of this decision.□

FOR THESE REASONS,□

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

-□

that the use of personal data obtained via the Crossroads Bank for Vehicles□

by customers of Informex SA, namely insurance companies, with a view to establishing□

personalized prices, constitutes a violation of articles 5.1 b) and 6.1 of the GDPR as well as□

of article 25 of the royal decree of 8 July 2013 implementing the law of 19 May 2010□

establishing the Crossroads Bank for Vehicles. The Litigation Chamber therefore orders□

to the defendant, in accordance with Article 58.2, d) of the GDPR and Article 100, § 1, 9° of the□

LCA, in its capacity as responsible for the processing of personal data□

above, to bring the processing into conformity within six months of the notification of the□

this decision and to inform the Litigation Chamber within the same period;□

pursuant to Article 100, § 1, 5° of the LCA, to issue a reprimand to the□

defendant following the violation of Articles 12, 13 and 14 of the GDPR, and□

to order the defendant, in accordance with Article 58.2, d) of the GDPR and Article 100, § 1,□

9° of the LCA, to bring the information he provides about his processing into compliance□

with Articles 12 to 14 inclusive of the GDPR, within three months of notification of this□

decision, and to inform the Litigation Chamber within the same period.□

-□

-□

*□

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

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

given as defendant.□

35 Omitting, however, the name of the defendant's data protection officer.□

Decision on the merits 34/2020 - 35/35

(Sr.) Hielke Hijmans

President of the Litigation Chamber