APPLYING THE EU GENERAL DATA PROTECTION REGULATION (GDPR) TO THE USE OF BANK CUSTOMER TRANSACTION DATA TO TRAIN AN AI BASED MARKETING MODEL: *A deeply defective and flawed decision of the Belgian data protection authority*

by

Douwe Korff

Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

11 April 2024

CONTENTS

1 Background 2

2 The facts 2

3 Applicable rules (main selected rules) 4

3.1 Purpose specification and -limitation 4

3.2 Transparency 4

3.3 Legal bases for the processing 5

3.4 The right to object: 7

3.5 The taking of automated individual decisions 7

3.6 The obligation to carry out a data protection impact assessment (DPIA) 8

4 Defects in the DPA decision 8

4.1 The DPA appears to have failed to ask for or examine relevant documents 9

4.2 The DPA did not clarify what data are covered by “transaction data” 10

4.3 The DPA did not really clarify what is meant by “data models” 12

4.4 The DPA did not check whether the processing involved the taking of automated individual decisions 13

4.5 The DPA did not sufficiently address the question of whether the data subjects were adequately informed 14

4.6 The DPA did not properly address the consequences of objections to the receiving of direct marketing offers 15

4.7 The DPA confused the issues of compatibility, transparency, legal bases and the right to object 15

5 Conclusion 19

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University
Associate, Oxford Martin School, University of Oxford

APPLYING THE EU GENERAL DATA PROTECTION REGULATION (GDPR) TO THE USE OF BANK CUSTOMER TRANSACTION DATA TO TRAIN AN AI BASED MARKETING MODEL:

A deeply defective and flawed Belgian decision

1 Background

On 15 March 2024, the Dispute Resolution Chamber of the Belgian Data Protection Authority (hereafter: the DPA) issued a decision under the EU General Data Protection Regulation (GDPR) on the use, by a bank, of the transaction data of its customers to build direct marketing data models.[1] The complainant in the case, a bank customer, had objected to the use of his transaction data for the training of the models.

Below, at 2, I set out the facts insofar as they can be gleaned from the decision.

At 3, I briefly summarise the legal standards that should have been applied in the case. I then show, at 4, that the DPA ignored or failed to properly apply many of them. At 5, I set out my conclusion.

2 The facts

The facts, insofar as they can be gleaned from the decision are as follows:[2]

The bank uses the transaction data of its customers, not just to carry out the relevant transactions (i.e., make the relevant payments, calculate interest, etc.), but also to underpin a separate, optional service called "personalised discounts" (*gepersonaliseerde kortingen*) relating to banking and insurance products and services. Bank customers are asked to sign up to ("activate") this discount service in a "digital application" (*digitale toepassing*), i.e., in an app.[3] If they do, they will then receive such offers; if not, they will not receive them. They can also withdraw their consent for the service, and in that case, they will no longer receive the offers.

The discount offers (and presumably, the decisions on whether to make a discount offer at all) are based on what are referred to in the decision as "data models" (*datamodellen*).[4] Notably, the bank will use the transaction data of both individuals who do sign up to the service and of individuals who have never signed up to the discount service to train the "data models" – unless the individual objects to this, as the complainant had done.[5]

[1] Geschillenkamer van de Gegevensbeschermingsautoriteit, Beslissing ten gronde 46/2024 van 15 maart 2024, Dossiernummer: DOS-2019-05837 (hereafter: "**the decision**"), available at:
https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-46-2024.pdf
NB: The decision is provided on the above page in Dutch. All translations into English of text from this report, and of text from the Big Data Report mentioned in footnote 12, below, are my own.

[2] As noted in the text (and even already in the next footnote), many facts are dispersed in different paragraphs and parts of the decision and often only obliquely noted.

[3] For some reason, the "digital application" (app) is only mentioned way into the decision, in paras. 42 and 45. The DPA does not appear to have examined the app in any detail: see below, at 4.1.

[4] I will discuss the nature of these "models" – which can be better described as "profiles" generated by AI – in my analysis at 4.3, below.

[5] The complainant had apparently never "activated" the discount offers service, i.e., had not signed up to it: see para. 9 of the decision. This rather important policy – to exclude the data of objectors from the training data – is only somewhat obliquely mentioned in the decision, e.g., in relation to the question of whether the complainant still

The bank has a privacy notice (*privacyverklaring*) that presumably is brought to the customer's attention when they first become a customer and/or is accessible through a link in the app or in an online banking site of the bank (although that is not explicitly clarified: see below, at 4.5).

The bank's marketing practices, and the information on the bank's marketing practices in the privacy notice, have changed over time:[6]

- The privacy notice of 2 February 2017 stated that the bank would use the customers' transaction data also "*to get to know its customers better and to use [their transaction data] for all the marketing and commercial purposes listed in the privacy notice*", which apparently made "*explicit reference to the purpose pursued by the [bank] to operate as a company and to the purpose of direct marketing of the banking and insurance activities of [the bank] and of the banking and insurance products or services of partners of [the bank]*" (para. 29). It would appear that these "partners" are separate entities, i.e., third parties in terms of the GDPR (see Art. 4(10) GDPR), although the DPA appears to have overlooked that: see below.
- The privacy notice of 1 September 2019 (that replaced the 2017 one and that apparently still applies)[7] states that the bank will use the customers' transaction data [also] "*to build analytical data models for commercial purposes*", but again limited to the marketing of banking and insurance activities (para. 30). However, "*from that moment it is said*" (I assume, in the privacy policy – DK) that "*[the] data models are made to make offers to the [bank's] customers of products and services of third parties*" (para. 31).

Later on, the DPA clarifies that the privacy notice was amended in September 2019 "*because of the preparation of the offering of personalised discounts of third parties, and therefore prior to this being initiated*" (para. 49). That ignores the fact that prior to September 2019, under the previous privacy notice, goods and services of "partners" – who must also have been third parties within the meaning of the GDPR – were also already being offered. But I will leave that aside.

In addition, the bank informed its customers of the "personalised discount" service by letter dated 21 September 2021, which according to the decision:

> informed [the bank customers] of the various aspects [of the processing] listed in Article 13(1) GDPR, by referring [them] to the amended privacy notice (para. 49).

The letter also informed the bank customers that they had a right to object (*idem*).

I will discuss the privacy notice and this letter in section 4.5, below, where I conclude that it is doubtful whether they really provides all the information that must be provided under Article

had an interest in the issue once "*the personal data of the complainant [were] no more contained in the overall dataset on which the models are to be based and trained*", and whether his objection had been complied with (para. 22); and later in relation to the question of "legitimate interest", as discussed below, at 3.3 and 4.6. It may well be that the "policy" was really a one-off and only adopted in response to the objection raised by the complainant in the case, and only applied in his case, but I will leave that aside. I will assume that the policy is now generally applied by the bank, in relation to any objector.

[6] The decision only discusses the privacy notices and marketing practices under the two notices listed in the text. What happened before that is unclear. The text in quotation marks are my translations of what the decision says about these notices. I am assuming that this is effectively what the actual notices said, [pretty much] *verbatim*.

[7] In para. 30, the decision refers to "the privacy notice of 1 February 2019", but this must be an error: all other references are to either the February 2017 one or the September 2019 one.

13(1) GDPR to data subjects when data are obtained from them. And at 4.6, I discuss whether the bank properly implements the right to object (I conclude it does not).

3 Applicable rules (main selected rules)

3.1 Purpose specification and -limitation

Under the GDPR, personal data must be:

> collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')
>
> (Article 5(1)(b) GDPR)

The issue of whether the bank's marketing and model training activities were compatible ("not incompatible") with the primary purposes for which it collected the transaction data is central to the case, as noted and discussed in some detail at 4.7, below.

Here, it will suffice to note that direct marketing by a company to its own customers on the basis of its own customer data (so-called "proximity marketing") is generally regarded as a compatible ("not incompatible") use of the data, at least if the goods or services that are marketed to those customers are similar to or closely linked to the goods and services generally offered by the company. On the other hand, disclosing (selling) of a company's customer data to another company so that that other company can use those data to offer its goods or services to the customers of the first company (so-called "third party marketing") is generally regarded as an incompatible purpose.

3.2 Transparency

When personal data are collected from the data subject (as is the case here), the latter must always be informed of the following (unless the data subject already has this information):

> (a) the identity and the contact details of the controller … ;
>
> (b) the contact details of the data protection officer, where applicable;
>
> (c) the purpose<u>**s**</u> of the processing for which the personal data are intended as well as the legal basis for the processing;
>
> (d) where the processing is based on [an assertion by the controller that the processing "is necessary for the purposes of the legitimate interests pursued by the controller or by a third party" (Article 6(1)(f), discussed below, at 3.3], the legitimate interests pursued by the controller or by a third party;
>
> (e) the recipients or categories of recipients of the personal data, if any; and
>
> (f) whether the controller intends to transfer the data to a third country.
>
> (Article 13(1) GDPR, slightly edited)

Note the plural in point (c): data subjects must be informed of *all* the purpose<u>**s**</u> for which their data are to be used, including any compatible ("not incompatible") purposes.

"Recipients" include "*[any] natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not*" (Article 4(9)).

Moreover:

> In addition to [the above information], the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing [including]:
>
> …
>
> the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
>
> (Article 13(2)(f))

Article 22 regulates "*automated individual decision-making, including profiling*" that "significantly" affects data subjects. I discuss this at 3.5 and 4.4, below.

When the data are collected directly from the data subjects (as is the case here), they must be given this information "*at the time when personal data are obtained*" (Article 13(1), initial sentence).

Moreover, the EU data protection authorities recommend that the information is provided in a "layered" way, with a simple up-front notice supplemented with further detail in a leaflet or (online) on another webpage.[8]

Note also the requirement under Article 7(2) GDPR, discussed in the next sub-section, to inform data subjects whose consent is sought for processing of their data for a not-necessary secondary purpose of that purpose "*in a manner which is clearly distinguishable from the other matters*", i.e., clearly separated from and distinct from the information on the primary purpose.

I will address the question of whether the bank's privacy notice and letter, in the form set out above, at 2, met the Article 13 and Article 7(2) requirements below, at 4.5.

All the above details should also be set out, in detail, in the record of processing activities (ROPA) that controllers must create in relation to any of their personal data processing operations (see Article 30 GDPR). But the DPA does not appear to have been asked for the relevant ROPAs; at least, they are not mentioned anywhere in the decision: see below, at 4.1.

3.3 Legal bases for the processing

All processing of personal data must have a legal basis. Those are listed in Article 6 GDPR and include, insofar as relevant for the present case:

> (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;

[8] See Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679 (WP260rev.01), issued on 22 August 2018.

> (b) processing is *necessary* for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> …
>
> (f) processing is *necessary* for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
>
> (Article 6(1)(a), (b) and (f), emphases added)

But the latter legal basis ("legitimate interest") cannot be invoked in relation to the processing of "special categories of personal data" (so-called "sensitive data"), i.e., of:

> personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
>
> (Article 9)

The legal bases, where they do apply, are moreover subject to further conditions and exceptions.

Thus, as concerns **consent**, the GDPR stipulates, first of all, that:

> 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
>
> (Article 4(11), in effect setting out the conditions for when consent can be regarded as valid)

Consent for the processing of sensitive data (as to which, see at 4.2, below) must moreover be "explicit" (Article 9(2)(a)). This also applies to consent to the taking of automated individual decisions, discussed in the next sub-section).

Article 7 expands yet further on the requirements for valid consent. It stipulates the following:

> *Article 7*
>
> **Conditions for consent**
>
> 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
> 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
> 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

> 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

3.4 The right to object:

In relation to processing of non-sensitive data based on the "**legitimate interest**" legal basis,[9] the GDPR stipulates first of all, quite generally, that

> The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on [the "legitimate interest" legal basis],[10] including profiling based on [that legal basis]. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
>
> (Article 21(1))

Moreover:

> Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing [and] [w]here the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
>
> (Article 21(2) and (3))

Note that unlike Article 22(1), the latter paragraphs are not limited to processing on the basis of the "legitimate interest" legal basis.[11] This is relevant in relation to secondary processing for direct marketing purposes: it means that even if the processing for the primary purpose is based on consent, or a contract, or even law, and even though some direct marketing (in particular proximity marketing) may well be compatible ("not incompatible") with that primary purpose (as noted above, at 3.1), if a data subject objects to this secondary processing, that processing should still end: "*the personal data shall no longer be processed*" for that secondary (and compatible) purpose. The same applies if direct marketing was the primary purpose (typically, if someone voluntarily gave their data to a direct marketing company, e.g., in a survey): if subsequently that data subjects no longer wants their data to be used, the data may no longer be used for that purpose (note that it does not suffice to merely not send marketing offers to the objectors).

The DPA does not appear to have taken this adequately on board, as I will notice below, at 4.6.

3.5 The taking of automated individual decisions

Article 22 GDPR stipulates the following:

Article 22

Automated individual decision-making, including profiling

[9] As noted earlier, the use of sensitive data cannot be based on the "legitimate interest" legal basis.

[10] Or on the legal basis that the processing is "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller", but that is not relevant here.

[11] Or on the legal basis mentioned in the previous footnote.

> 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
>
> 2. Paragraph 1 shall not apply if the decision:
>
> (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
>
> (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
>
> (c) is based on the data subject's explicit consent.
>
> 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
>
> 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

The DPA completely ignored this issue, although it is important, as discussed below, at 4.4.

3.6 The obligation to carry out a data protection impact assessment (DPIA)

Article 35 adds to the above *inter alia* that:

> A data protection impact assessment … shall … be required in the case of:
>
> (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
>
> (b) processing on a large scale of special categories of data referred to in Article 9(1) ...

In the decision, the DPA also did not address the question whether these provisions might apply in the case at hand. I will discuss this at 4.1, below.

4 Defects in the DPA decision

The parties' arguments and the DPA decision focussed on: (i) whether the use of the bank customers' transaction data for (a) the training of the data models and (b) the making of "discount offers" was compatible ("not incompatible") with the primary purpose for which those data were processed, i.e., the making of the relevant transactions and associated actions (like calculating interest or bank charges); and (ii) what the legal bases might be for the use of the transaction data for the training of the data models and for the making of the offers. (Note that the separation and separate treatment of the two secondary purposes – the training of the models and the making of the offers – is crucial to the DPA's analysis and based on a report on "Big Data" produced by that DPA.)[12]

I will come to those issues below, at 4.7. However, presumably because the parties did not, or not clearly, raised them, the DPA ignored or failed to clarify a range of issues that in my opinion have great bearing on the issues that were addressed.* The DPA also failed to check the existence of – and therefore also failed to examine – crucially important mandatory documents. These failures amounted to a lack of due diligence on the part of the DPA and seriously affected the resulting decision. I will address those non-addressed matters first, at 4.1 – 4.6 At 4.7, I will take a critical look at the confusing way in which the issues that were addressed were addressed.

* **NB:** Some might argue that because some issues were not raised by the parties, the DPA was not under any obligation to address them. However, that argument is dismissed by the DPA itself in the section in which it addresses the argument of the bank that the case is inadmissible because the complainant no longer has an interest at stake, now that the bank stopped using his data for the training of the data models (para. 9). The DPA dismisses this on the ground that the right to complain has a wider aim: to ensure compliance with the law more generally; and that the DPA has a broad mandate to investigate issues arising from a complaint (see paras. 17 – 22). The DPA therefore could, and in my opinion should, have looked at the broader issues, also taking into account relevant matters not explicitly raised by the parties. In any case, as I hope I am showing with this short analysis of the decision, the DPA could not properly address the identified issues without also looking at the non-identified and non-addressed ones, and at some crucial documentation.

4.1 The DPA appears to have failed to ask for or examine relevant documents

The DPA does not appear to have asked for or looked at the mandatory **records of processing activities (ROPAs)** that the bank is supposed to have drawn up in relation to the processing for the various purposes (primary purpose: carrying out the transactions and associated activities such as calculations of interest, etc.; secondary purpose of marketing of discount offers; and the purpose associated with that – as discussed below, at 4.7 – : the training of the data models) (See Article 30(1)). Or at least, they are not mentioned anywhere in the decision. The bank would have had to make the relevant ROPAs available to the DPA on request (Article 30(4)).

The DPA also does not appear to have looked more broadly at the data that are collected and processed in the **app**. Did the app collect data on its use? On the locations of the user? Even without actually examining the app itself, this could and should have been clarified by looking at the relevant mandatory (!) ROPAs.

Furthermore, because the DPA appears to have not even considered whether the processing involved in the creation of the profiles might involve the taking of "significant" automated individual decisions (as discussed at 4.4, below), the DPA also does not appear to have considered whether the bank was required to carry out a **data protection impact assessment (DPIA)** – as is required "in particular" in the cases of:

> (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions

[12] Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL), Big Data Rapport, 2018 (?), p. 34, available at: https://www.gegevensbeschermingsautoriteit.be/publications/big-data-rapport.pdf
See also the illustration and further detail on p. 35.

> are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
>
> (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10.
>
> (Article 35(3)(a) and (b))

Note that even if it were to be argued that (contrary to my view) the profiling and marketing by the bank (and third parties) did not involve the taking of automated decisions, the transaction data still contained sensitive data (see at 3.3, above, and 4.2, below) and, given that the transaction data of all the bank's customers (except for the data of the rare objectors) were used to these ends, the processing of the transaction data can clearly be said to take place "on a large scale".

The record of such a DPIA must contain *inter alia*:

> (c) an assessment of the risks to the rights and freedoms of data subjects … ; and
>
> (d) [a description of] the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.
>
> (Article 35(7)(c) and (d))

In particular, it is well-known that AI-based models will often show **biases** that can lead to discrimination against, e.g., ethnic or religious minorities – especially if there are biases in the data used to train the models/generate the relevant profiles. A proper DPIA record would show (a) whether the bank had tried to ascertain if there were such biases in the models or the training data; (b) what measures, if any, it had taken to minimise or remove them; and (c) how effective those measures had been.

By not even addressing whether the profiling by the bank amounted to individual decision-making (as discussed below, at 4.4) or involved processing of sensitive data on a large scale, and thus also ignoring the – in my opinion clear – duty on the part of the bank to carry out a DPIA, the DPA again simply ignored a major issue relating to the protection of individuals in the digital environment, and failed to look at crucial documentation.

4.2 The DPA did not clarify what data are covered by "transaction data"

This is actually crucial. In particular, although the words may sound innocuous, a bank customer's full transaction data will inevitably be highly revealing: it can show (to give but a few examples):

- ➢ that a person is a member of a political or religious organisation or trade union (e.g., when they pay a membership fee by standing order, or make regular or irregular payments to such an organisation);
- ➢ payments to a straight or gay sexual information or porn site – thus revealing the customer's sexual orientation;
- ➢ payments to an abortion clinic or for a wheelchair or dialysis machine or hearing aids – thus revealing information on the customer's health;

In other words: "transaction data" will inevitably include "special categories of personal data" ("sensitive data") as defined in Article 9(1) GDPR (quoted above, at 3.3), that in principle prohibits the use of such data (subject to limited exceptions).

The DPA only refers to sensitive data in its assessment of the impact of the processing on the data subjects in the context of its assessment of "legitimate interest" as a legal basis, where it observes that:

> None of the documents in the case indicate that special categories of personal data within the meaning of Article 9 GDPR are processed **in the data models**. (para. 46, emphasis added)

This is both non-sensical and disingenuous. It is non-sensical because, of course, no personal data – and therefore also no sensitive data – are processed "**in** the models": the models are statistical (possibly dynamic) algorithms. As the DPA itself clarifies:

> [A]ccording to [the bank] the models [that are the result of the training] are simply and only algorithms that no longer contain personal data, and the [DPA} has [seen] no proof to the contrary (para. 46)

The real questions are:

- *are any sensitive data (e.g., the kinds of information listed above) used in the creation and subsequent training (refining) of the models?*

The DPA did not address or check this, even though its own Big Data Report (on which it relied and to which it repeatedly expressly refers in its decision) specifically gives as examples of the kinds of data that may be extracted from large data sets (such as a bank's database of the transactions of [all] its customers): "*credit-worthy or not; presence of an illness or not; interested in a specific product or not, …* ".[13]

Note that while financial data, and in particular data on credit worthiness are not explicitly listed as "special categories of personal data" ("sensitive data") in the GDPR, it is recognised that they should still be treated with special care, precisely because they are so revealing and sensitive in a broader sense.

- *do the models result in the making (or non-making) of offers to selected individuals (customers who have signed up to the "personalised discount" service) on the basis of established or inferred sensitive characteristics of those individuals? Or even: does their application inadvertently result in such discrimination?*

This is crucial because profiling is notorious for resulting in bias and discrimination – and processing of personal data that results in discrimination is inherently unfair and therefore in violation of the basic "lawfulness and fairness" principle in the GDPR (Article 5(1)(a)) and therefore unlawful.[14]

[13] Big Data Report (previous footnote), p.35 (clarification of the illustration of the two-phase processing involved in Big Data data mining, discussed in the text below).

[14] I discuss this in some detail in my paper AI & the GDPR (forthcoming), section 3.3.1, at iii, *The use of AI that results in discrimination*.

The failure of the DPA to even look at these issues is disingenuous (to say the least). I will return to this in section 4.7., below.

4.3 The DPA did not really clarify what is meant by "data models".

The DPA decision does not go into any detail as concerns the data models (*datamodellen*), beyond making clear that they form "*the basis for the offering of the personalised discounts*".[15] However, the DPA does note (in para. 46 of the decision) that the bank creates its "data models" essentially in the way described in its Big Data Report, i.e., in phase one of a two-phase process. It is worth looking at the description of both those phases in that report:[16]

> In the first or preliminary phase one can create and train a mathematical model on the basis of **as-much-as-possibly anonymised data** from which at least the direct identicators have been removed. Furthermore, **in this phase, one can use, store and** consider [read: **analyse** – DK] **all data on any variables (including the class labels [i.e., labels attached to a category of data subjects in the data set, such as "good employee"/"bad employee"]**[17] **that are available (of course on condition that those data are lawfully processed), for training and possible inclusion in the ultimate model.**
>
> In the second phase (the phase that involves "singling out" and/or identification of the data subject)[18], that involves the operational application of the model that was trained in the previous phase, only the data/variables may be used, collected [read: correlated?] and stored that had been shown in the training phase to significantly contribute to the predictions of the model (principle of minimisation of data processing).

Two things stand out. First of all, the reference to "*as-much-as-possible-anonymised data*". This is a misleading phrase. Data can be identifiable, or pseudonymised (in which case they should still be treated as identifiable: see recital 26 to the GDPR that makes this explicitly clear), or anonymised, i.e., incapable of being re-identified.[19] "*As-much-as-possible-anonymised data*" are, put simply, not completely anonymised data. In other words, they should be treated as, at best, pseudonymised data – and therefore, for the purposes of the GDPR, as personal data.

That in itself completely destroys the clear suggestion in the report that, secondly, controllers are free to feed any data they hold into the data model training data sets – with the caveat in brackets, "*of course on condition that those data are lawfully processed*", actually begging the

[15] See, e.g., para. 22 that refers to "*the buidling of the data models on the basis of which the personalised discounts are offered*" ("*het bouwen van de datamodellen op basis waarvan de gepersonaliseerde kortingen worden aangeboden*").

[16] Big Data Rapport (footnote 12, above), p. 34, paragraph break and emphases added. See also the illustration and further detail on p. 35 of that report.

[17] See the Big Data Report (footnote 12, above), p.27.

[18] The footnote added to the above (footnote 150 to the report) refers to a margin note (*randnummer*) to a decision of the DPA on a draft decree relating to energy fraud (see footnote 148 to the report). Presumably, this in turn refers to recital 26 to the GDPR that clarifies that if a person can be "singled out" from a group of people or from a data set, even without being identified by name, that person should still be regarded as "identified" for the purposes of the GDPR.

[19] See my paper on The requirements of the EU General Data Protection Regulation (GDPR) relating to the processing of pseudonymised and anonymised data (and other perhaps not immediately identifiable data): A complex issue (forthcoming).

very question that should be asked: ***when is it lawful to do this?*** I will come to that question below, at 4.7, in relation to the question of the legal bases for the processing by the bank.

Here, it must be noted that the whole point of the "data models" is to evaluate personal aspects of the individuals who have signed up to the "personal discount" service, by means of the data models, in order to put a "class label" (or several such labels) on them: "*likely to be interested in and able to afford [a particular banking or insurance product or service]*" or "*unlikely to be interested in/unlikely to be able to afford [the product or service]*".

In other words: **the data models are profiles.**

Cf. the definition of "profiling" in Article 4(4) GDPR:

> 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Such profiling is increasingly – in practice, by now almost universally – done by means of artificial intelligence (AI).

More specifically, therefore: it must be assumed that the bank's direct marketing "data models" are profiles created with the use of AI.

This has major implications in terms of the GDPR that are again effectively ignored by the DPA, as again further discussed at 4.7, below.[20]

4.4 The DPA did not check whether the processing involved the taking of automated individual decisions

As noted above, at 3.5, Article 22(1) GDPR in principle prohibits the taking of decisions "based solely on automated processing, including profiling, which produces legal effects concerning [the data subject] or [which] similarly significantly affects him or her."

Often, receiving (or not receiving) a direct marketing offer will have no legal or otherwise significant effect on the recipient (or on the person not receiving the offer). However, the financial and insurance sector is special in that regard. If an AI system determines, on the basis of an analysis of my bank transaction data (and the profile that generates) that I will be offered a special "discount" mortgage or credit card rate, but that my neighbour will not be offered that special (lower) rate, it can at least be argued that the offer has "significant" effects (on me, positive ones, in that it presumably saves me significant amounts of money; on my neighbour, negative ones).

[20] The use of profiles also has major implications in terms of the recently adopted AI Act that stipulates, in Article 6(3), final sentence, that "*an AI system referred to in Annex III shall always be considered to be high-risk where the AI system performs profiling of natural persons*." Annex III covers *inter alia* AI systems used in the context of access to and enjoyment of essential private services (such as banking – DK) including "*AI systems intended to be used to evaluate the creditworthiness of natural persons or establish their credit score*" (with an exception of AI systems used for the purpose of detecting financial fraud, but that is not relevant here). Given that the DPA decision was issued shortly after the AI Act, the DPA might at least have mentioned and considered it. But I will leave this aside for now.

This applies *a fortiori* if the profiles in effect amount to credit scores. The DPA did not look into this.

Nor did the DPA seek to ensure that – if the offers involved the taking of automated decisions or profiles with significant effect – those decisions or profiles were not based on sensitive data (see above, at 4.2), or if such data were used, that "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests" had been put in place (see Article 22(4) GDPR).

I will return to this issue, too, at 4.7, below.

4.5 The DPA did not sufficiently address the question of whether the data subjects were adequately informed

The DPA appears to accept (without making much of this) that prior to the September letter, the bank customers were not adequately informed of the secondary (direct marketing) use of their transaction data (see para. 28). But I will leave that aside and limit myself to the September 2019 privacy notice and letter, noted at 2, above.

As noted there, the decision simply states, without any detailed analysis, that the bank customers were informed of "*the various aspects of the processing listed in Article 13(1) GDPR*" (listed above, at 3.2), by means of the letter they were sent, that referred them to the amended privacy notice (para. 49).

The customers will indeed have been aware of the identity and contact details of the bank that were presumably printed on the letter; and the letter or the privacy notice may also have mentioned the bank's DPO and their contact details. But it is more doubtful whether the letter and the notice were sufficiently specific about the secondary purpose(s) of the processing, and about the categories of recipients of their data.

Specifically, the privacy notice informs customers that their transaction data will be used "*to build analytical data models for commercial purposes*" and (if they sign up to the "personalised discount" service) "*to make offers [of banking and insurance products and services] of third parties to [them]*".

In my opinion, this does not make it clear to the bank customers that the processing involves the creation of (AI-based) profiles on them. Non-technical data subjects cannot be expected to realise that that is what the reference to "*building analytical data models*" means (although the DPA disingeuously claims everyone would realise this: see below, at 4.7).

Similarly, all that is said about the recipients of the "data models"/profiles is that they are "third parties" and that they offer goods and services relating to banking and insurance. In my opinion, that too is insufficiently precise.

There is also no indication in the decision that the bank "*explicitly brought to the attention*" of the bank customers their right to object to the secondary processing; or if this was mentioned, that this was "*presented clearly and separately from any other information*" (see Article 21(4)).[21]

[21] Note that there is also no indication in the case that the complainant objected to the processing of his transaction data for the creation of the data models/profiles because he learned about this right from the letter or the privacy notice; presumably, he simply knew about this right otherwise.

More importantly, the DPA failed to even consider whether any of the information listed in Article 13(2) GDPR – and that should be provided if this is "*necessary to ensure fair and transparent processing*" – should have been provided. In particular, if (as I believe to be the case) the creation of the data models and the offering of third party goods and services on the basis of the models involved the taking of "significant" automated individual decisions, the bank customers should have been informed of this.

4.6 The DPA did not properly address the consequences of objections to the receiving of direct marketing offers

The complainant in the case specifically objected to the use of his transaction data for the creation and training of the data models/profiles – and this objection was complied with in that the bank moved his transaction data from the training data. It must also be assumed that this is a general practice by the bank: that if anyone objects to this specific use of their transaction data, those data will no longer be used for this training of the models.[22]

But all too often, companies that are involved in direct marketing respond to objections from data subjects by simply removing them from the relevant mailing lists, while continuing to use their data to train their marketing models/profiles. They claim to thereby have complied with requests "to not receive any further marketing communications" from the company concerned. Often, links sent with marketing offers use precisely those words: "If you no longer want to receive offers from us, please click here". It is only when a data subject very specifically objects to the processing of their personal data for the marketing that they will remove the objector's data from their training data (as was done here), because the GDPR demands that (in response to such a specific objection): see section 3.4, above.

The DPA does not appear to have checked how – aside from the case of the complainant, who was clearly knowledgeable about the GDPR – the bank generally treats requests from individuals to no longer receive direct marketing offers. If the bank in question followed the common practice noted above, I would not be surprised if it responded to such requests by removing the individuals from the mailing lists used to send the "personalised discount" offers – but without ending the use of their transaction data in the training of the models/profiles.

4.7 The DPA confused the issues of compatibility, transparency, legal bases and the right to object

The DPA treats the creation and training of the data models/profiles and the making of personalised discount offers by third parties as two separate (secondary) purposes, distinct from the primary purpose of the carrying out of the relevant transactions. It thus concludes in relation to the former (which it says corresponds to the "first phase" of Big Data data use described in its Big Data Report) that:

> The creation of data models in order to offer personalised discounts for products and services of third parties to [bank customers] is a new purpose that must be distinguished from the initial purpose, i.e., the carrying out and recording of payments. (para. 31)

[22] See footnote 5, above.

And as noted below, the DPA held that this processing can be based on the "**legitimate interest**" legal basis.

By contrast, the DPA agrees with the argument of the bank that the use of the "data models"/profiles to actually make offers to bank customers who have signed up to the "personalised discount" service (the "second phase") must be assessed separately under the GDPR; and that this use can be and is based on the **consent** of the subscribers to the service (para. 47).

As noted earlier, the DPA assessed the "legitimate interest" issue without first checking whether sensitive data are used in the creation and training of the models[23] (as will almost inevitably be the case) or whether the processing involved the taking of automated individual decisions (as I also believe to be the case) (see above, at 4.2 and 4.4, respectively) – in which cases the "legitimate interest" legal basis simply could not be relied on. That is in itself a major defect in the decision.

That aside, in its analysis of the "legitimate interest" issue, the DPA referred to the *Rigas* judgment of the Court of Justice of the EU, in which the Court held that:[24]

> Article 7(f) of Directive 95/46 lays down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence.

The DPA held that the bank had a commercial interest in "*the digitalisation and personalising of [its] services and diversification of the range of [its] offers*", and thus a legitimate interest in building the data models: it met the first condition (para. 40, with reference to the WP29 Opinion on the issue).[25]

The DPA also held that the "*data analysis of the transaction data is a necessary means to the intended purpose, i.e., the offering of digital applications for the offering of personalised discounts to [the bank's] customers*", i.e., it also met the second condition.[26]

For the DPA, the issue therefore came down to the third condition: whether an appropriate balance had been struck between the above-mentioned legitimate interests of the bank and the rights and interests of the data subjects, i.e., the customers. It held that such a balance had been struck, taking into account (a) "the normal expectations of [bank customers]" and (b) a series of parameters relating to this "first-phase" processing (the creation of the models/profiles).

[23] It disingenuously said that no sensitive data were included "**in** the models: see at 4.2, above.

[24] CJEU, judgment of 4 May 2017 in Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'* (*Rigas*), ECLI:EU:C:2017:336, para. 28, quoted in para. 38 of the decision.

[25] WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217), adopted on 9 April 2014.

[26] "[D]ata-analyse van de transactiegegevens voor het trainen van modellen [vormt] een noodzakelijk instrument … om het uiteindelijk beoogde doel, namelijk het aanbieden van digitale toepassingen voor het aanbieden van gepersonaliseerde kortingen aan klanten van de verweerder, te kunnen realiseren." (para. 42)

On the first point, according to the DPA:[27]

> it is within the normal range of reasonable expectations of complainant (read: bank customers generally) that the defendant (the bank) will use their transaction data – unless complainant (read: a bank customer) objects [to this] – to train data models (without further using these operationally to offer personalised discounts, for which consent is requested).

Also relevant in the assessment of whether the right balance had been struck were, in the view of the DPA, a range of other matters noted in the same paragraph:[28]

> In this, the defendant (the bank) may only use data from which as many identifying particulars have been removed as possible in order to train a model, an algorithm, without that model in this phase being applied operationally to identified individuals.
>
> No attempts may ever be made to re-identify the individuals in the data – to the extent that this might still be possible after the removal of as many identifying particulars as possible.
>
> Moreover, according to the defendant (the bank), the models that are created are only and simply algorithms that no longer contain any personal data, and [the DPA] has no proof to the contrary.
>
> Also to be taken into account is [the fact that] at no time are personal details of customers passed on to third parties.
>
> In addition, there is no evidence in the case materials that special categories of personal data within the meaning of Article 9 GDPR are processed in the models.

This is an odd mix of supposed legal requirements "*the defendant may only …* "; "*no attempts may be made …*"); assertions by the bank, some of which are dubious, that are nonetheless unquestionably accepted by the DPA; and misleading wording.

Thus, there is no clarification as to how compliance with the requirements ("*may only*"; "*may not*") is ensured.

Thus, if the bank passes on an offer from a third party to a bank customer who is identified by the relevant "data model" as meeting certain criteria (e.g., savings of more than a certain amount), and the customer responds to the offer, the third party will have been informed of the fact that that customer met those criteria (some of which may even relate to sensitive characteristics of the data subject).

[27] "[Het valt] binnen het normale verwachtingspatroon van de klager … dat de verweerder zijn transactiegegevens gebruikt - behoudens verzet van de klager - om datamodellen te trainen (zonder deze verder operationeel te gebruiken voor het aanbieden van gepersonaliseerde kortingen, waarvoor toestemming wordt gevraagd)." (para. 46.)

[28] "De verweerder mag hierbij enkel gegevens verwerken waarbij zoveel mogelijk identificatoren van betrokkenen zijn verwijderd om een model, een algoritme, te trainen zonder dat dit model in deze fase in een operationele context wordt toegepast op geïdentificeerde personen. Er mogen bovendien nooit pogingen worden ondernomen om – als dat nog mogelijk zou zijn na het verwijderen van zoveel mogelijk identificatoren van betrokkenen – de personen in de trainingset te heridentificeren. Ook zijn volgens verweerder de resulterende modellen enkel en alleen algoritmen die geen persoonsgegevens meer bevatten, en de Geschillenkamer heeft geen bewijs van het tegendeel. Daarbij dient ook in rekening te worden gebracht dat op geen enkel ogenblik persoonsgegevens van klanten worden doorgegeven aan derden. Daarenboven blijkt uit geen enkel stuk dat er bijzondere categorieën van persoonsgegevens in de zin van artikel 9 AVG in de datamodellen worden verwerkt." (para. 46, paragraph breaks added)

And as already noted at 4.3, above "a*s-much-as-possible-anonymised data*" (here referred to as "*data from which as many identifying particulars have been removed as possible*") are, put simply, not completely anonymised data. In other words, they should be treated as, at best, pseudonymised data – and therefore, for the purposes of the GDPR, as personal data.

And the reference to there not being any sensitive data "**<u>in</u>** the data models" is equally misleading and disingenuous, as already noted at 4.2, above.

Also, as already noted at 4.5, above, in my opinion it does not "*fall within the normal range of reasonable expectations*" of bank customers that their highly private and revealing complete transaction data are used by their bank to create direct marketing models for third parties.

Yet on the basis of this mish-mash of odd "findings", the DPA concludes that:[29]

> [The impact of the use of his transaction data to create and train models] on the complainant is therefore extremely minor, with the processing of his personal data reduced to a minimum in the sense that while it is true that his data are used, but without this leading to the offering of personalised discounts to the complainant in the phase of the building of the models when the complainant has not given his express consent for this.
>
> Moreover, the complainant can at any time exercise his right under Article 21 GDPR to object to the use of his data for the building of the models [as a means to] the offering of personalised services of this parties.

Any actual offering of third-party goods or services is only done in relation to customers who have subscribed to the "personalised discount" service. Therefore, there are "no further consequences" (*geen verdere gevolgen*) for customers such as the complainant, who have not signed up to the service, from the use of their transaction data in the data models (para. 47).

And:[30]

> All of the above elements leads the [DPA] to conclude that the third condition [for the application of the "legitimate interest" legal basis] has also been fulfilled and [the bank] can therefore rightly invoke the legal basis of Article 6(1)(f) GDPR for the building of data models in order to offer personalised discounts for products and services of third parties. This incompatible secondary processing is therefore lawful.

The false suggestion noted in section 4.3, above, that controllers are effectively free to feed any data they hold into the data model training data sets they want to use for direct marketing clearly flows from this same line of thinking.

[29] "De Geschillenkamer is dan ook van oordeel dat de impact op de klager dus uitermate gering is en de verwerking van zijn persoonsgegevens tot een minimum is beperkt in die zin dat zijn gegevens weliswaar worden hergebruikt, maar in de fase van het bouwen van de modellen geen aanleiding geven tot het aanbieden van gepersonaliseerde kortingen indien de klager daartoe niet zelf actief toestemming verleent. Bovendien kan de klager ook altijd zijn recht van bezwaar uitoefenen tegen het gebruik van zijn gegevens voor het bouwen van de modellen voor het aanbieden van gepersonaliseerde kortingen van derden in de zin van art. 21 AVG." (still para. 46, paragraph break again added).

[30] "Het geheel van bovenstaande elementen brengt de Geschillenkamer tot het besluit dat ook aan de derde voorwaarde is voldaan en de verweerder zich dus terecht beroept op de rechtsgrond van artikel 6.1 f) AVG voor de bouw van datamodellen met het oog op het aanbod van gepersonaliseerde kortingen voor producten en diensten van derden, waardoor deze onverenigbare verdere verwerking als rechtmatig moet worden beschouwd." (para. 48)

5 Conclusion

The various defects in the DPA decision, noted above:

- the failure to check whether the training data contained sensitive data or whether the AI-based offerings amounted to significant automated individual decisions;
- the lack of clarification about the legal requirements (“*may only*”; “*may not*”);
- the use of misleading terminology (“a*s-much-as-possible-anonymised data*”); and
- the over-easy bank-friendly acceptance of bank customers’ supposed “reasonable expectations” –

in my view alone suffice to regard the decision as fundamentally flawed.

However, the most fundamental error on the part of the DPA lies in the separation of the two elements of the processing: the “phase one” building of the models and the “phase two” application of those models to allow third party marketing, and the treatment of these two phases as, effectively, two separate processing operations for two supposedly separate purposes.

This is a sleight of hand that allowed the bank to claim, and the DPA to accept, that the processing in the two phases can be treated separately under the GDPR: under this approach, “phase one” (the creation and training of the models) is seen as a purpose in itself, and because bank customers are supposed to “reasonably expect” that the bank will do this, and suffer no consequences from it (unless they voluntarily sign up to the “personalised discount” service), this can be based on the “legitimate interest” legal basis, although the processing in “phase two” (the actual making of the discount offers by third parties) cannot be based on “legitimate interest” but requires consent.

It is perfectly reasonable to describe the bank’s activities (and similar activities of other entities facilitating direct marketing) as a two-phase process. But it remains one process, for one purpose: direct marketing. The DPA itself accepts that:[31]

> The use of [complainant’s] transaction data in the data model [must be regarded as] … purely an interim step towards the ultimately pursued purpose, i.e., the offering of personalised discounts.

But in that case, the “interim step” requires the same justification, the same legal basis, as the overall process: consent.

The DPA’s splitting off of “phase one” from the overall process, and allowing it on a separate legal basis, is either a fundamental conceptual error or – if done deliberately to “help” the bank in its monetisation of its customers’ transaction data – deceitful.

Hopefully, further decisions by other DPAs, and ultimately the Court of Justice, will rectify this gross error.

- o – O – o -

Douwe Korff (Prof.)   Cambridge (UK), 11 April 2024

[31] “[H]et gebruik van zijn transactiegegevens in het datamodel [dient te worden beschouwd] … louter als een tussenstap voor het uiteindelijk beoogde doel, het aanbod van gepersonaliseerde kortingen.”