Relevant circumstances of the case:

- The organisation that was fined is the Dutch national tennis association. A non-profit responsible for all professional and leisure tennis in the Netherlands.
- They are fined €525.000,- Which is the first GDPR fine in the Netherlands.
- KNLTB is fined for two GPDR violations:
    1. Incompatible processing with regard to the purpose of collection of pre-2007 members: art. 5(1)(b)
    2. Processing without a legal ground of members who joined since 2007: art. 5(1) and art. 6(1)
- KNLTB has 570.000 members.
- KNLTB has since 2007 generated extra revenue by sharing personal data with sponsors for direct mail. Since 2018 the association has also shared personal data for telemarketing. Both telemarketing and direct mail are opt-out channels in the Netherlands, having mandatory Robinson Lists.
- The DPA investigation started in October 2018, after the KNLTB announced it would share personal data of members with sponsors for tennis-related and other promotions. The DPA received an undisclosed number of complaints. One member, a lawyer, took legal steps to prevent sharing of his data. He also sought access to a national media outlet, which in the wake of GDPR made a television item about it. In this item the chairman of the DPA appeared for comment, where he declared that the KNLTB did not act in accordance with the GDPR since consent was required to share data with third parties.
- Subject of the investigation is the transfer of personal data to two advertisers:

1. Advertiser A received a file for direct mail with:
    a. first and last name
    b. address
    c. city
    d. postal code
    e. gender

    This transfer was covered by an agreement, which contained (among other things) the restriction of the use to two mailings per year, mandatory cleaning with the Robinson list, and previous approval of the KNLTB

2. Advertiser B received a file for telemarketing, which would be used to call on behalf of the KNLTB to promote subscriptions of the advertiser. The file contained:
    a. gender
    b. first and last name
    c. addres
    d. city
    e. date of birth
    f. postal code
    g. phone number
    h. e-mail address
    i. tennis club

    This campaign was the only telemarketing campaign, it was cancelled on the request of KNLTB because there were too many complaints.

- The shared data files did not contain data of minors or any special categories of personal data.

Steps taken by KNLTB to ensure GPDR compliance

- Sponsors who received data needed to conclude an agreement stating the conditions for use of the data, mandatory technical security measures, retention, etc.
- In 2007 the member assembly agreed with the use of names and addresses for direct mail by KNLTB sponsors to generate extra revenue. This was deemed necessary to deal with the declining number of members, and to keep tennis affordable in the Netherlands. The alternative was to raise the contributions of members. The members have been informed about this at the time.
- In 2017 the board of KNLTB wanted to expand their mandate to share member data. The request to allow sharing data with sponsors for telemarketing was approved by the member assembly and communicated accordingly.
- As of 2015 members receive welcome-emails, since 2018 privacy is a topic in this email. The information contains a paragraph explaining the direct marketing activities mentioned above, including a reference to a contact form with an opt-out. The webpage also states that e-mail addresses will only be shared with consent.
- In 2018 multiple dedicated newsletters went out, specifically to inform about direct marketing activities by KNLTB, also referring to the opt-out form.
- After the media attention the KNLTB put up a special message on the homepage and several big tennis-related websites to once again inform their member-base.

Assessment by the DPA

- Transfers to third parties for direct marketing of members before 2007 are considered ‘further processing’ of data which was collected on the legal ground ‘fulfilment of the membership agreement’. Processing will be assessed on compatibility with this original purpose. If incompatible, another legal ground is necessary, either consent or a legal obligation. (DPA refers to p. 19-20 of WP29 opinion 09/2013 on purpose limitation)
- Member data of members who joined KNLTB after 2007 will be considered to be also collected for the purpose of direct marketing. Therefore the assessment will be made whether the legal basis is valid. This is not considered ‘further processing’

1. Members <2007

Is the purpose of generating additional revenue compatible with the purpose of fulfilling the membership agreement? This is assessed according to the five criteria of article 6(4) GDPR. The DPA states that there is no link whatsoever between both purposes.
Regarding the reasonable expectation of data subjects KNLTB argues that members have been informed many times, and it has been explained that all generated revenue directly benefits all members by supporting the sport and keeping it affordable. The DPA states that it must be assessed whether the processing was within the reasonable expectations of the members. They argue that becoming a member of KNLTB is non-optional if you join any tennis club in the country. There is no choice whether to provide personal data, since it is necessary for the agreement. Because of this mandatory character members can be considered to expect that their data would only be used for the purpose it was collected for. Informing does not change the expectation at the time of data collection, since the information came after collecting.

The fact that the telemarketing campaign was cancelled due to complaints is an indicator that it was not within reasonable expectation. The DPA also points out that e-mail addresses were shared for a telemarketing campaign, while the KNLTB clearly stated to members this would only happen after consent.

The DPA argues that the distribution of member data leads to a loss of control for the data subject. Providing an opt-out cannot be considered to be a mitigating measure, since this is legally required. The fact that the revenue benefits members does not take away the loss of control.
As an aggravating factor the DPA mentions that the telemarketing campaign entailed the distribution of 314.478 records, where only 39.478 were called after a selection by the advertiser. According to the DPA this involved a risky processing of a large number of records without it being necessary.
The KNLTB points out that the marketing campains had a high conversion, which would lead one to believe that members appreciate it. But the DPA highlights that the majority was either not called, or did not show an interest. And receiving a promotion mailing or telemarketing call is something that can be perceived as a nuisance. In this argument the fact that both channels have a robinson list appears not to be taken into account.

Conclusion: A violation of 5 (1)(b), for incompatible processing. Since there is no link between both purposes, it is not within the reasonable expectation, the consequences for members and the lack of mitigating measures. The KNLTB should have asked consent.

2. Members >2007

The DPA considers that its conclusion that a legitimate interest should be traced back to a fundamental right or legal principle follows from the system of the GDPR. Any processing of of personal data is an interference with the fundamental right to data protection. As a result, any processing is initially unlawful. This follows from article 6(1) GDPR, which states that a processing activity can be lawful if there is a legal basis.

The GDPR provides a legal basis to processes personal data, which consists of six legal bases. Here the DPA highlights the conditions under which a controller can rely on legitimate interest. For a valid appeal on legitimate interest, three conditions must be met:

- a legitimate interest of the controller or a third party
- necessity of the processing for the interest pursued
- the rights and freedoms of the data subject should not prevail

<u>Legitimate</u>

The interest at stake must qualify as ‘legitimate’. This entails that the interest is named in (general) legislation or elsewhere in law as a legal interest (rechtsbelang). It has to be an interest that is protected by law, which is considered worth protecting, which must in principle be respected and enforceable.

The controller or a third party must be able to appeal to a (written or unwritten) legal rule (rechtsregel) or legal principle (rechtsbeginsel). If this legal rule is:

- sufficiently clear
- accurate
- sufficiently predictable

the processing can take place on legal basis c or e (legal obligation or public interest).

But there are also cases where the legal rule or legal principle regarding the processing of personal data is not (sufficiently) clear and accurate, and/or the application is not (sufficiently) predictable. In these cases there can nevertheless be a legitimate interest for the controller or a third party. There interests should at all times be *real, concrete and direct,* not *speculative, in the future or derived.* It can in principle any material or immaterial interest.

The sole interest to generate money or profit with personal data in itself does not qualify as a legitimate interest. Not just because an interest like that usually isn't sufficiently specific -in a certain sense everyone always has an interest in having more money- but in a more principle way also because this would lead to the assumption that it is allowed to balance this interest. A balancing between:

- The sole, non legally/by law (juridisch/rechtens) protected interest a party has in optimally monetizing someone's personal data on one hand, and on the other hand:
- the constitutionally entrenched interest a data subject has regarding his or her data protection.

The GDPR legal bases of consent and the agreement have only a few limitations regarding commercial opportunities. The difference with legitimate interest is, that the latter entails processing without the will of the data subject. This is the domain where the rights of the controller clash with the fundamental rights of the data subject. The idea that it would in principle be allowed to make a profit by choosing to infringe someone fundamental rights is incompatible with the principle of control by the data subject. Such a wide margin for a balancing of interests cannot be the intention of the GDPR, and isn't named , allowed or advocated by the EDPB (reference to opinion 06/2014 on legitimate interest)

The legitimacy of the interests (also according to WP29) is crucial for the question whether the threshold is reached by the controller to be allowed to balance a certain interest. The phase of the balancing (both necessity and the balancing test) isn't reached if the interest cannot be deemed 'legitimate'. If the controller cannot appeal to a legally/in law protected interest (the data subject always can), there is nothing to balance. The other way around this means that the protection from a closed system of legal bases would easily be undermined if the sole interest of monetizing data would be considered legitimate. Then under certain circumstances it would be easy to argue that the income is necessary to achieve the interest of maximizing profit. Then only a material balancing is required by the controller with a commercial interest, between the controller making money, and interfering someone else's fundamental rights. In an extreme case this would lead one to argue that, as the potential profit increases, the interference with fundamental rights could equally be increased. This evidently is not intended with GDPR, The fundamental right to data protection would become an illusion.

The freedom of entrepreneurship is recognised in the EU Charter of Fundamental Rights to recognise the contractual freedom and the freedom of competition. This is of course not unlimited, but only 'conform union law, national law and practices'. This right give entrepreneurs the freedom to choose whom they do business with, and determine their own prices, etc. It is not the case that this general fundamental right gives the right to make money (as much as possible) in itself. It also doesn't create the situation that 'being able to

make less profit' would lead to a clash with the fundamental right to privacy or data protection of someone else. Entrepreneurs on the other hand do for example have a duty of care regarding employees and/or customers. These duties have been regulated in specific or general legal norms. Fulfilling these duties can be considered to be a legitimate interest.

The information above leads to the situation that legitimate interests have a more or less urgent and specific character which follows from a (written or unwritten) legal rule or legal principle. It must be (in some sense) be unavoidable that this interest is pursued. Reference to an ECJ case:

[36] Zie bijvoorbeeld het arrest van het Europese Hof van Justitie van 4 mei 2017, ECLI:EU:C:2017:336, r.o. 29: '[...] dat het belang van een derde bij het verkrijgen van persoonsgegevens van degene die schade heeft aangebracht aan zijn eigendom, teneinde de schade op deze persoon in rechte te verhalen, een gerechtvaardigd belang is'. Zie in die zin het arrest van het Europese Hof van Justitie van 29 januari 2008, ECLI:EU:C:2008:54, r.o. 53).
[37] WP29 Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46EC", p. 25.

This also follows from, albeit in other words, from the WP29 opinion on legitimate interest: *"Accordingly, an interest can be considered as legitimate as long as the controller can pursue this interest in a way that is in accordance with data protection and other laws. In other words, a legitimate interest must be 'acceptable under the law"*

Conclusion: The reasoning above leads the DPA to the conclusion that the interest of the KNLTB to transfer personal data of members with sponsors for direct marketing was not legitimate. As a result there is no legal basis.

3. Separate point regarding data transfers to third parties: regarding art. 6(4) the DPA clarifies its position, being that this 'further processing' assessment limits to further processing by the controller within its own organisation. For data transfers to third parties a controller needs a separate legal basis.