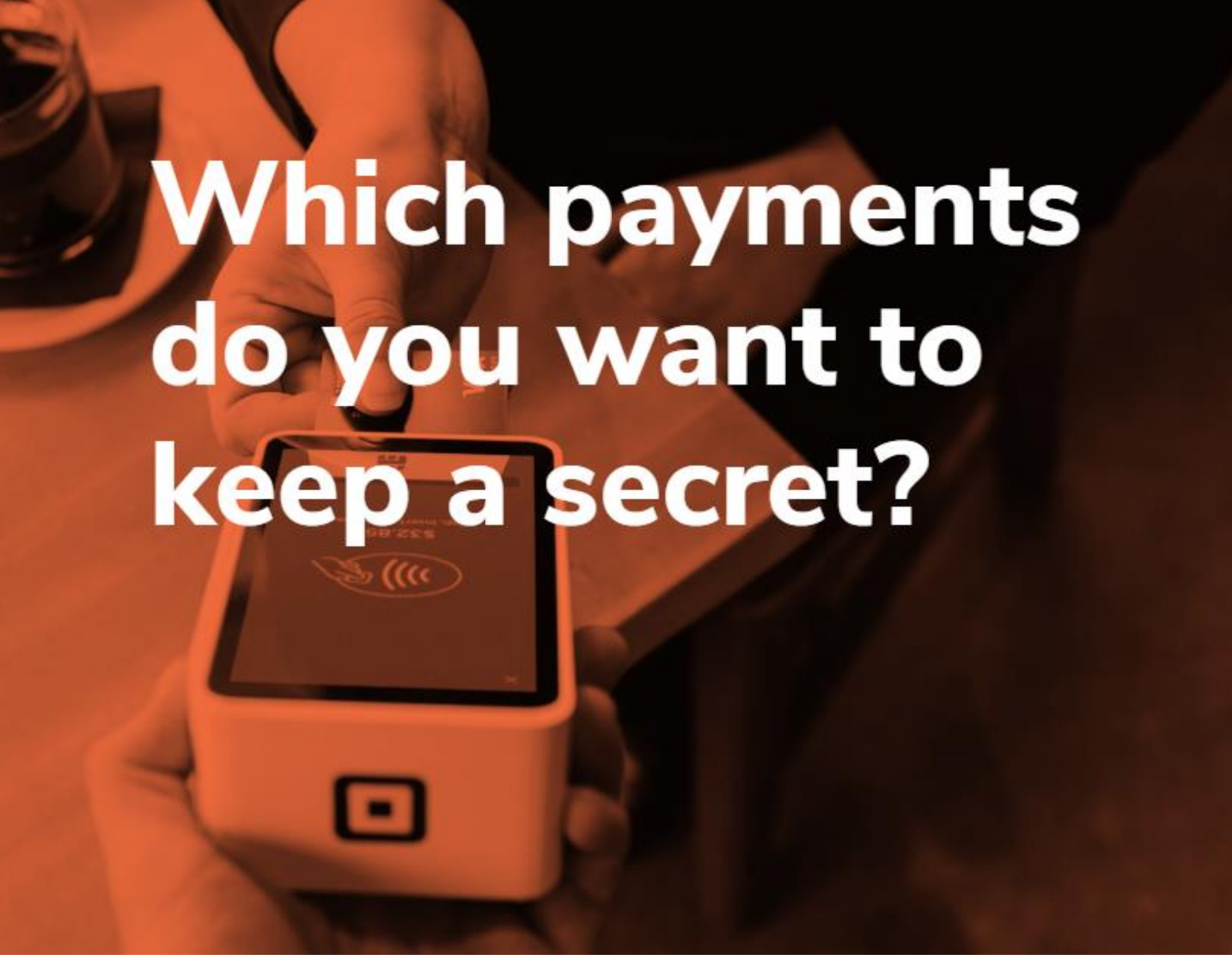


PSD2 ME NIET

This whitepaper on PSD2 and privacy
is an initiative of

PRIVACY FIRST
your choice in a free society

Whitepaper PSD2 and GDPR
May 2021, version 1.0

Privacy First Foundation
P.O. Box 16799
1001 RG Amsterdam
The Netherlands
Tel. 0031 20 810 0279

Why this whitepaper?

The key to innovation in the financial sector lies with companies that take up the challenge of combining innovation with privacy. The protection of the personal data of consumers is crucial for a privacy-friendly future. In this whitepaper, we outline the main challenges to privacy created by the second Payment Services Directive (PSD2) and shed light on the solutions that are already available today.

We address this whitepaper to all parties which are or may become involved in the matters we describe. All account information service providers (AISPs) entered in the European Banking Authority (EBA) register and relevant stakeholders will receive this whitepaper.

About us

First, let us introduce ourselves. We are the Privacy First Foundation, a Dutch foundation that was founded in 2008 and is committed to preserving and promoting the right to privacy, as well as the personal freedom and liberty in the private sphere. It is registered as having a charitable status (ANBI).[1]

Privacy First is a constructive partner; we seek solutions for privacy risks and encourage organisations to invest in privacy protection. One example of our efforts is the annual Dutch Privacy Awards where we showcase privacy-friendly solutions for businesses, consumers and public authorities.

As an NGO that promotes civil rights and privacy protection, we have been concerned with financial privacy for years and since 2017, we have been keeping close track of the developments surrounding PSD2, pointing out the dangers to the privacy of consumers as data subjects. In particular, we focus on privacy issues that arise around 'account

[1] Privacy First is recognized as a non-profit, public interest foundation (Algemeen Nut Beogende Instelling – ANBI). Amsterdam Company Register No. 34298157.

information service providers' (AISPs) and the possibilities offered by PSD2 to further process personal data.

As in 2017, we thought that providing more adequate information and more transparency to consumers would be sufficient. However, the risks associated with PSD2 turned out to be greater and more fundamental. We therefore launched a bilingual (Dutch & English) website called PSD2meniet.nl/en in order to outline both our concerns as well as our solutions with regard to PSD2. Through this project we wish to contribute to making positive improvements to PSD2 and its implementation in order to achieve enhanced protection of personal data. With our Don't-PSD2-Me-Registry[2], a 'privacy filter' based on this registry and a number of best practices, we believe we can make great strides towards achieving better protection.

Please feel free to contact us on this whitepaper or on the solutions we mention. Or read our input on the guidelines to see what is on our mind.[3]

We wish your business every possible success. It would be wonderful if you could make your operations privacy friendly by adopting the solutions offered in this whitepaper. Naturally we are always available to clarify our recommendations. Finally, we would once more like to refer to our website PSD2meniet.nl/en for additional information about our project and activities.

Kind regards,

Vincent Böhre
Privacy First Foundation Director
Vincent@PrivacyFirst.nl

Martijn van der Veen
PSD2 spokesperson
Martijn@PrivacyFirst.nl

[2] https://psd2meniet.nl/en/

[3] 'Our response to the PSD2&GDPR guidelines', https://psd2meniet.nl/en/onze-reactie-op-de-richtlijnen-over-psd2gdpr/

Content

AISPs process personal data

The European Data Protection Board (EDPB) adopted the 'Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR' on 15 December 2020. The EDPB has emphasised that transaction data that flow from and to natural persons are personal data and are therefore subject to the General Data Protection Regulation (GDPR).

Special categories of personal data

Financial transactions may reveal sensitive information about individual data subjects, including information that falls into special categories of personal data as defined in the GDPR.[4] For example, depending on the transaction details, political opinions and religious beliefs may be revealed by donations made to political parties or organisations, churches or parishes. Trade union membership may be revealed by the deduction of an annual membership fee from a person's bank account. Personal data concerning one's state of health may be gathered through the analysis of medical bills paid by data subjects to medical professionals (for instance psychiatrists). Finally, information on certain purchases may reveal information about a person's sex life or sexual orientation.

Even a single transaction may contain information appertaining to special categories of personal data.

Account information services might rely on profiling as defined by article 4(4) GDPR. As stated by the Article 29 Working Party in the Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as endorsed by the EDPB, "profiling can create a special category of data by inference from data which is not a special category of data in its own right, but becomes so when combined with

[4] Article 9(1) GDPR

other data."[5] This means that, through the sum of financial transactions, different kinds of behavioural patterns can be revealed, which may include special categories of personal data. Therefore, the chances are considerable that service providers processing information on financial transactions of data subjects also process special categories of personal data.

Article 9(1) GDPR prohibits the processing 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".

These data may only be processed if one of the exceptions as laid out in a non-exhaustive way in Article 9(2) applies. Most likely, the only exception that will effectively apply is the one related to data subjects giving explicit consent. This exception sets requirements for giving consent, for informing data subjects about the processing of their personal data and for the legitimacy of doing so.

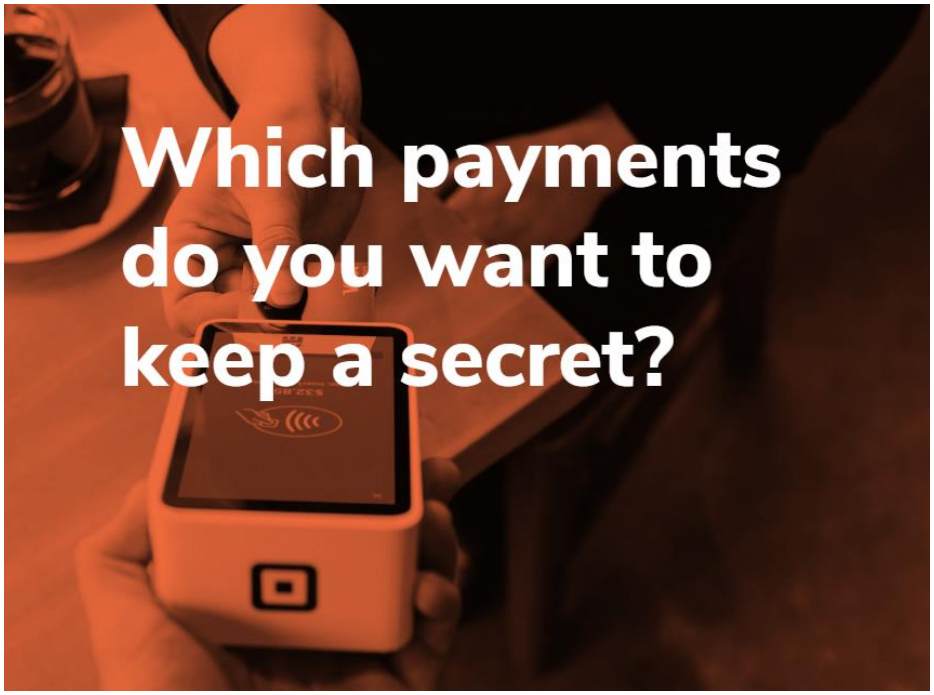
If the conditions for the basis of 6(1)(a) 'consent' in Article 7 GDPR are not met, a fine upwards of €20 million or 4% of the worldwide turnover of an AISP may be imposed. The unlawful processing of special categories of personal data may result in the imposition of the same fine.

Processing special categories of personal data can pose a significant compliance and business risk to AISPs. However, our concern is that AISPs do not sufficiently protect their customers and expose them to risks of unauthorised use of their personal data, for example by revealing their sensitive data unintentionally and against their will.

Consumers cannot limit the amount of financial data shared once they have given their consent. At this moment, even if a financial services provider does not need certain data, all data are shared after consent has been given. This is contrary to the principle of data minimisation under

[5] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, page 15.

the GDPR. If such a simple filter does not exist, what can one expect from the protection of special categories of personal data?



Risks

The risks of processing

There are two instances when account information service providers pose a risk to the privacy of their customers that can only be mitigated through active intervention by AISPs. The first instance is when AISPs engage other parties to process and categorise the data and use these for profiling. The second instance is when AISPs aim to sell additional services, for example by offering to provide budget management services or through personalised offers being made based on payment behaviour. If credit scoring or risk assessment is part of these processes, it is very likely that personal data will be added to customers' profiles.

The most significant risks we perceive are the following:

- Consumers cannot filter and restrict the use of data. Following the request for and the granting of consent, simply all data are shared. Consumers are not in control and are dependent on service providers for data minimisation;

- Special categories of personal data are not protected. At the moment, there is no way of filtering such data and yet they are provided to parties who are not allowed to process them;

- Consumers are not informed sufficiently and accurately. They may receive the legally required information without understanding the scope, risks and purpose of data processing. Pages or documents containing explanatory information are too lengthy, too complex and are not suitable for giving explicit consent to.

EDPB: Full control over personal data must be the objective

The EDPB states that "certain questions and concerns in respect of the *need* that the data subjects remain *in full control* of their personal data [emphasis added by Privacy First]." This places the responsibility with the data controller, i.e. AISPs. Unfortunately, it is clear from our experience

that the GDPR and all related laws, regulations and elaborations are not adequate to achieve this goal. The GDPR will have to be interpreted in such a way that it effectively benefits data subjects. This may take a far-reaching form of Personal Data Management (PDM) to give data subjects full control, up to the point where they are no longer dependent on the efforts and privacy friendliness of AISPs.

There are already good technologies and applications that effectively allow data subjects to process their data by use of a smartphone. For example, we point to initiatives such as 'the Financial Passport' (Financial Passport Foundation[6]) or the 'rental passport' (Qii[7]). Under PSD2, access to one's own data should be made possible as a matter of principle.

Data subjects are barely able to exercise their rights, partly due to the fact that consumer profiles are constantly being supplemented with data. Once a data subject's data are processed by an AISP and this AISP involves other parties in the processing, it will be virtually impossible for an individual to have an understanding of the processing of their data or the deletion thereof. Even if an individual is successful in obtaining such insight, their profile will be enriched with data regardless. With PSD2, profile enrichment will be even easier and will have a greater impact than the processing of separate data that are being collected now.

Are your customers at risk?

With regard to data protection, in accordance with Article 94(1) PSD2, any processing of personal data, including the provision of information about the processing, for the purposes of PSD2, shall be carried out in accordance with the GDPR.

When personal data are processed for the purposes of PSD2, the exact purpose of the processing should be specified, the applicable legal basis should be named, the relevant security requirements laid down in the GDPR must be implemented, and the principles of necessity, proportionality, purpose limitation and proportionate data retention periods must be respected. Also, data protection by design and data

[6] https://financieelpaspoort.nl/

[7] https://qii.nl/

protection by default should be embedded in all data processing systems developed and used within the framework of PSD2. Any deviation will increase the risk for the data subjects concerned.

In practice, there will be a significant difference between the level of protection offered by the PSD2 and the GDPR. Unfortunately, the level of protection of the GDPR appears to be lower than that of the PSD2. This is particularly relevant to AISPs that wish to provide additional services or process personal data further, in which case safeguards derive only from the GDPR. Violation of the GDPR can be sanctioned. However, it will not result in the withdrawal of the banking license and thus the cessation of operations, but instead in a relatively lower sanction, i.e. a fine upwards of €20 million or 4% of the worldwide turnover.[8]

Is your business at risk?

In our opinion, the greatest risks to the privacy of data subjects arise when AISPs start offering additional services, or when they start collaborating with third parties. This will involve new or expanding services and/or the further processing of personal data. Because there is already a commercial relationship, in these cases providers have more opportunities to influence the behaviour of their customers. Therefore, the threshold for sharing personal data will be lower and initial safeguards will be weaker, exacerbating existing risks.

Is your business at risk? And what about your customers?

The possibility of further processing data is described in sections 2 and 3 of the guidelines on PSD2 and GDPR, items 20 to 24. This possibility is the primary focus of our advocacy efforts and this whitepaper. Transaction data may be used for additional processing of personal data pursuant to Article 5(1)(b) and Article 6(4) GDPR. For AISPs, this is where the true promise of the PSD2 lies and new business models can emerge with transaction data as a raw material. The PSD2 offers the possibility of linking financial data with other data. Transaction data provide a complete and in-depth profile of data subjects.

[8] Article 83 GDPR

So, is your business at risk, you may wonder. That may well be worth taking a closer look at. Businesses may be at risk when they do not fulfil the objectives and obligations of the GDPR with regard to providing information, privacy by design, taking proper measures, processing personal data and special categories of personal data without proper consent. When your services remain strictly within the bounds of the definition of an AISP, without using third parties for profiling or providing services that require personal data, you may count yourself lucky. Otherwise, we suggest you read our solutions.

Solutions

With this white paper we contribute with solutions. We list a number of solutions that seamlessly fulfil the requirements of the GDPR and the Guidelines of the EDPB.

How to know if i process special categories of personal data?

The processing of sensitive personal data is allowed only if one of the grounds for exception of Article 9(2) of the GDPR applies. Often, the only exception will be the granting of consent by data subjects. Consent must be granted in a specific way and on the basis of adequate information. Before AISPs can inform data subjects and give them the opportunity to grant consent, they will first have to detect the possible presence of sensitive personal data. In its guidelines, the EDPB provides a number of examples of transactions from which special categories of personal data can be derived. We will show how easy it is to detect the account numbers involved.

Solution: Find account numbers of organisations involved

In order to detect sensitive personal data, the bank account number linked to the data must be known. We show how to find these accountnumbers.

Sensitive personal data can often be linked to organisations one-on-one. Whether or not organisations process sensitive personal data depends primarily on what category organisations belong to.

In the European Union, organisations are categorised according to the industry standard classification system called NACE Rev. 2.[9] In the Netherlands, equivalent Standard Business Indicator (SBI) codes are used by Statistics Netherlands among others. By connecting organisations to categories of sensitive personal data, it is easy to identify which

[9] https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF

organisations are involved. These organisation can easily be found online as most of them have a public profile and provide public information on websites.[10]

According to Privacy First, organisations within at least the following categories process sensitive personal data and thus can easily be identified:

Political views
- 9492 Political organisations

Religious or philosophical beliefs
- 94911 Religious organisations

Membership of a trade union
- 9420 Trade unions

Health data
- 86 Health care. This section comprises:
  - 861 Hospitals
  - 862 Medical and dental practices
  - 869 Paramedical practices and other ambulatory health care
- 87 Nursing, care and guidance with overnight accommodation. This section comprises:
  - 871 Nursing homes
  - 872 Homes and day care centres for psychiatric patients and the mentally disabled
- 4773 Pharmacies

Dealing with sexual behaviour or sexual orientation

Data relating to a person's sexual behaviour or sexual orientation may be more difficult to detect. Sensitive personal data can be inferred from payments made or received, for example from or to certain organisations such as those representing the LHBTI+ community. The most prominent organisations in this field can easily be found.

[10] If a separate account exists for membership (fees) then only the affiliate account number will need to be recorded.

Dealing with personal data relating to criminal convictions and offences

With PSD2 there is a risk that a person's criminal profile can be derived on the basis of certain transactions. Transactions can be traced back to fines and may thus reveal criminal information. On the website of the Dutch Public Prosecutor's Office several violations and associated fines are listed. Fines and other transactions are transferred to one of the twelve publicly disclosed account numbers of the Central Judicial Collection Agency.[11] A transaction to one of these account numbers likely reveals data related to one's criminal offences.[12]

Although these personal data are not categorised as special, restrictions and additional conditions apply to their use.

This information can be used not only for profiling, it may circumvent existing, regulated practices, such as black lists.[13] Black lists must comply with formal requirements and security safeguards as well as the provision of general information on (the need of) processing personal data, as well as information on the inclusion of blacklisted data subjects. However, in combination with public information, basic profiles can be created on the basis of financial data, thereby circumventing the safeguards of the protection of fundamental rights and freedoms of the data subjects concerned. The processing of such data may easily be in breach of the GDPR.

[11] https://www.cjib.nl/rekeningnummer

[12] Even in case of more serious offences and crimes, fines provide a great deal of information. From the website 'Extract from judicial documentation' of Justid, the judicial information service' (https://www.justid.nl/organisatie/JDS/registratie.aspx) it can be deduced for which crimes fines are handed out in the Netherlands. In addition, for a large number of offences you will end up with a criminal record. The 'Besluit justitiële en strafvorderlijke gegevens' (https://wetten.overheid.nl/BWBR0016544/2018-01-01/#Hoofdstuk2_Afdeling1_Artikel4) lists which offences are by default included in one's judicial documentation (criminal record).

[13] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/register-zwarte-lijsten

Solution: detect by using Privacy First's Don't-PSD2-Me Registry

As part of our PSD2meniet.nl project, Privacy First has taken the lead in designing and establishing a Dutch Registry containing the account numbers of 'special account holders', demonstrating this can effectively be realised.[14]

Why not avoid problems with sensitive data?

The Don't-PSD2-Me Register is open for all AISPs willing to detect (and, at a later stage, filter) financial transactions which can be regarded as special categories of personal data. The registry can be used also by all NGOs, law enforcers and supervisory bodies willing to use these insights for their legal investigations. And last but not least, the registry can be used by every individual who wants either to check whether their financial transactions contain any special categories of data, or to execute their legal rights as data subjects.

In case you would like to provide services in The Netherlands, please contact us for more details.

Solution: Collaborate and urge the EU and the EDPB to introduce an independent and neutral registry

In our view, there is a need for a neutral way of determining whether financial transactions should be regarded as special personal data. Such a provision does not yet exist.

In our response to the open consultation on PSD2 guidelines in 2020, we urged the European Commission (EC) and the EDPB to take the initiative of creating an independent and neutral register of account numbers, in which it is laid out that transactions by or to account holders can be regarded as sensitive personal data.

You could contribute to this registry and demand for it. On this we are on the same side.

[14] https://psd2meniet.nl/gezocht-rekeningnummer-voor-het-register/

How to deal with data minimisation and data protection by design and default

In its guidelines, the EDPB elaborates extensively on privacy by design and data minimisation. Privacy by design is a system development philosophy based on the idea that privacy should be taken into account throughout the entire development lifecycle of a system, from its inception, through implementation and deployment, all the way to the moment when the system is decommissioned and no longer used.

The EDPB writes: "When not all payment account data are necessary for the provision of the contract, a selection of the relevant data categories should be made by the AISP before the data are collected."

"In this respect, the possible application of technical measures that enable or support Third Party Providers (TPPs) in their obligation to access and retrieve only the personal data necessary for the provision of their services could be considered, as part of the implementation of appropriate data protection policies, in line with article 24(2) GDPR. In this respect, the EDPB recommends the usage of digital tools in order to support AISPs in their obligation to only collect personal data that are necessary for the purposes for which they are processed. For instance, when a service provider does not need the transaction characteristics (in the description field of the transaction records) for the provision of their service, a digital selection tool could function as a means for TPPs to exclude this field from the overall processing operations by the TPP."

TL;DR?

In short: Implement privacy by design

The GDPR also sets out the obligations to apply data protection by design and by default. Article 25 reads: "Controllers shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are *necessary for each specific purpose of the processing are*

processed [emphasis added by Privacy First]. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility."

The principle of data minimisation is enshrined in Article 5(1)(c) GDPR: "Personal data shall be […] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed". Essentially, under the principle of data minimisation, controllers should process no more personal data than necessary in order to achieve the specific purpose in question.

At the moment, a major problem is that consumers cannot independently limit the amount or filter the processing of their bank data. Even if a financial services provider does not need certain data, all data are shared once consent is given. Subsequently, a consumer has no guarantee whatsoever that a service provider will ensure data minimisation.

A consumer has no guarantee whatsoever that a service provider will ensure data minimisation.

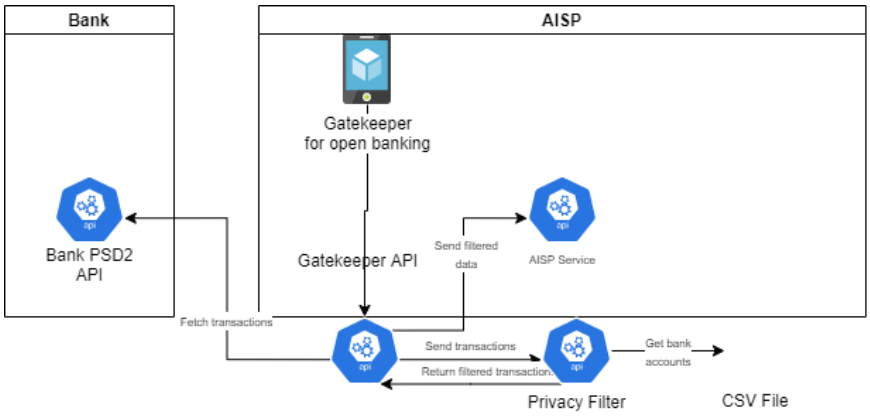
For many services, it is possible to determine in advance which personal data need to be processed. An example is a risk analysis for taking out a mortgage, where, for example, only an income statement over the past two years is required. For many other services that are often conveniently placed under the heading 'innovation', even the required data cannot be determined, or the aim of the AISP is simply to obtain the largest possible data set. 'First the data, then the thinking' is often the adage. Here Privacy First sees a substantial risk because this puts the principle of data minimisation in jeopardy.

By using services for further processing data such as credit scoring or other forms of risk indication, a third party can make an in-depth analysis of a person based on that information. Moreover, we do not rule out the possibility that AISPs will also use third parties, including credit rating agencies, for 'consolidated financial statements' while remaining within the definition of an account information service.

Solution: Don’t-PSD2-Me Filter / Privacy Filter by Privacy First

Under the PSD2 legislation, consumers cannot filter or restrict data. Even if they want to, or if a service provider indicates in advance that they do not need all the data. More difficult, we aim at removing or masking certain transactions, containing sensitive data. No such solution existed, so we build one.

The filter is simple in design and execution. And thus easy to implement. The Privacy Filter is a simple solutions, as the component diagrams shows.

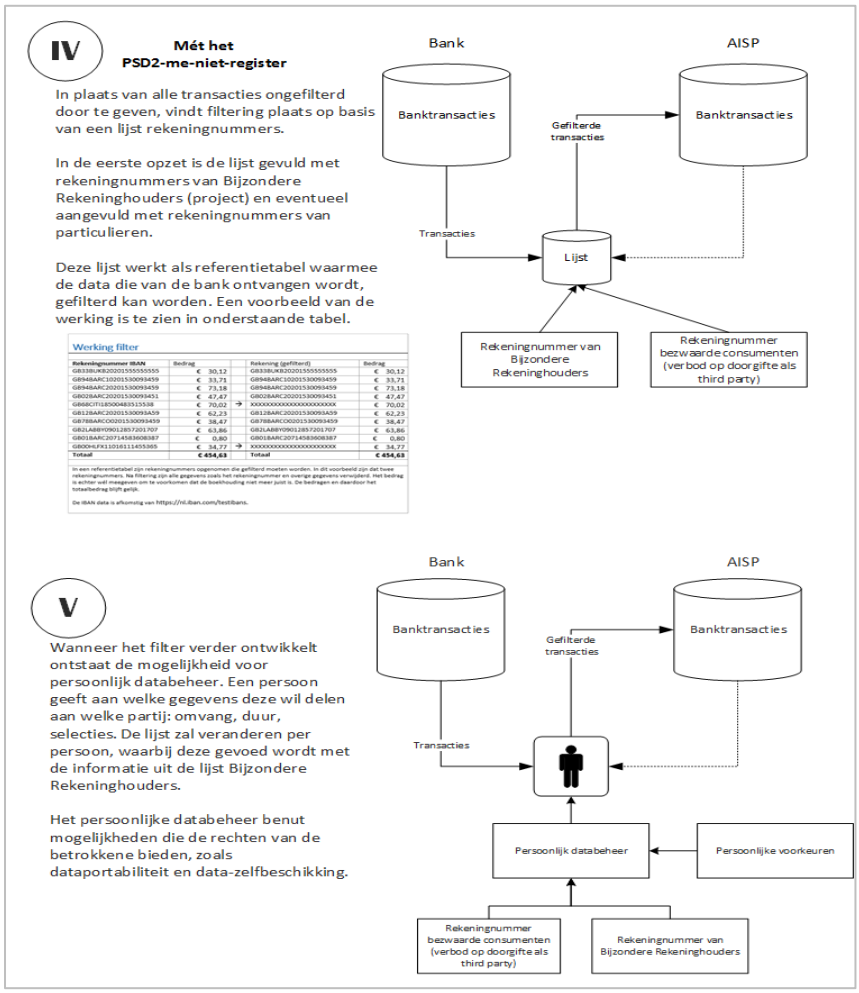


The Don't-PSD2-me Register provides a tool for PSD2 service providers to filter the received payment data. In short, the Don't-PSD2-me register is a list of account numbers, with which it must be possible to filter. The account number plays a central role in the register. This is the unique number with which transactions to or from a party can be found. We build the filter and collected account numbers which reveal special categories of personal data. We like to stress that filtering of masking these data will have limited impact of data shared.

At this moment, we collected over 300 account numbers of (national) political parties and organisations revealing political onions, account numbers revealing personal data revealing to criminal convictions and offences, account numbers of labour unions, the 60 largest organisations revealing religious beliefs and we are working on organisations in healthcare. Although we are aware this is no 100% score, at some

categories we score over 90% of the account numbers of the organisations processing special categories of personal data.

The Privacy Filter gives customers the choice to share sensitive data or not. It is part of our roadmap towards Personal Data Management (PDM).



Figuur 1: part of the conceptual model, the roadmap towards PDM

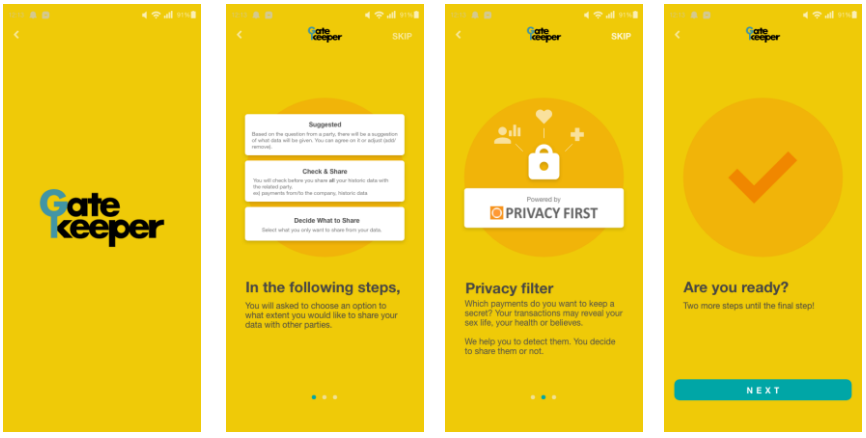
Solution: Gatekeeper for Open Banking (Privacy Filter included)

We contribute to the development of fintechs by adding our Privacy Filter in their solution. We do so to show the working of the detecting and filtering and offer AISP's the possibility to use this solution of the shelf.

Once party who incorporated the privacy filter is the Gatekeeper for Open Banking, a service of FwdPay, an innovative company focused on the development of services based on the PSD2. The Gatekeeper is being developed to become an intermediary between banks, AISPs and service providers, using technologies such as blockchain, zero-knowledge proofs and tools for the detection and filtering of special personal data. FwdPay and Privacy First are working together to develop the Privacy Filter in such a way that it can be easily used by AISPs.

We put in some screenshots to bring this solutions to life. The Gatekeeper enables safe sharing and enables data filtering as solutions for data minimisation. At this point, the customer can specify the level of detail he or she is willing to share.

At first, a customer opens the GateKeeper as an app provided by an AISP.

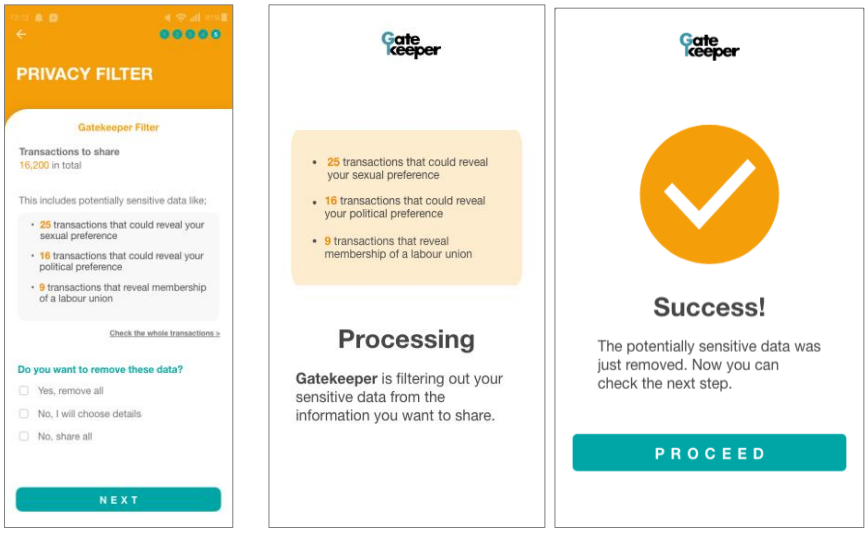


Figuur 2: Landing screens of the Gatekeeper app

At second, the customer selects options for limiting the level of detail and data shared. He can set his preferences from sharing all to a very limited

amount of data, depending on its preferences. The GateKeeper provides filter options for debet/credit, history, times for sharing (once to recurring) and can dive into depth.

The Gatekeeper will use the **Privacy Filter** to detect the special categories of personal data as mentioned before. The screenshot below shows the detected transactions. At this moment, a person should be informed on the processing and give its consent. At this point a person has the possibility to filter the data or share them.



Figuur 3: Screens of the Privacy Filyer: detect, filter, share

The last step is that the data is shared to the specific third party, while complying to privacy principles such as necessity, data minimisation and protection of the data subject. The consent and data transferred is logged. 100% compliant to the GDPR.

How to deal with transparency and accountability

In the GDPR, consent is defined as a "freely given, specific, informed and unambiguous indication of the wishes of the data subject with which, by means of a statement or clear positive act, they consent to the processing of their personal data." These four elements are essential for valid consent.

The intended effect of the GDPR is thus that a person can make an informed choice about the processing of their personal data on the basis of information. However, in the case of PSD2, this principle is undermined as the term 'informed' in the GDPR definition is generally misinterpreted by controllers as the need to simply provide data subjects with the legally required information. This basically means that in practice, the data subject is not 'informed' at all, because the scope of the consent given can no longer be overseen. The effect will be that, although data subjects know that consent has been given, they will hardly be able to indicate what the processing entails in scope and nature and what risks are posed to their fundamental rights.

Transparency and accountability are key elements of data protection. Currently, consumers are not properly and fairly informed as much of the information they are provided with is difficult to understand. This is a lamentable state of affairs, not least because a lot of value is attached to their explicit consent. But how much value does consent have if consumers cannot sufficiently assess the consequences of granting consent?

Informing customers is about their understanding, not you being compliant.

It is imperative to provide data subjects with adequate and easily intelligible (extensive background) information – possibly by means of bullet points – about which personal data are processed, how these are processed, and for what purpose. The provision of real-time notification of data may at times also be practical.

The call for clear information is not limited to financial information. Consumers who want to use AISPs share their data with third parties. This involves as much information as is available from the payment service provider, which essentially is a significant amount. With the push of a button, a person shares their complete financial history. Research by the Dutch Consumers' Association ('Consumentenbond') showed that Dutch

banks enable their customers to have access to their own data created, on average, over the past seven years. Some banks allow access to account statements that are up to two years old, while others do not limit the retention period at all, potentially offering an overview of a lifetime of financial transactions.[15]

We like to stress that service provides have to be careful when it comes to the degree by which persons voluntarily use a service. Using a link to PSD2 for credit assessments should be allowed only if providers ensure sufficient safeguards in the form of preventing profiling, not adding datasets to other, already collected information of the individuals concerned and strict data minimisation. Even under these conditions, the dividing lines between 'enticement', 'gentle coercion' and 'involuntariness' on the part of consumers is very thin.

One development generated by the PSD2 is that service providers will use other service providers under the PSD2 for their financial support. Tellingly, we learnt about the case of a treasurer of a sports association who wondered if he should agree to use a PSD2 service provider to collect dues. Investigations revealed that the sports association referred to the privacy statement of a third party, which in turn happened to be a reseller of the final processor. We expect to see more and more such schemes as service providers will purchase payment services from licensed parties. It will be impossible for the average data subject to get a clear picture of who is processing their personal data, which contravenes the principles of the GDPR.

Article 12 GDPR states that information should be provided in a concise, transparent, comprehensible and easily accessible form and in clear and simple language. Practice shows, however, that information is often not provided in accordance with these standards. Privacy statements are too long and difficult to fathom.

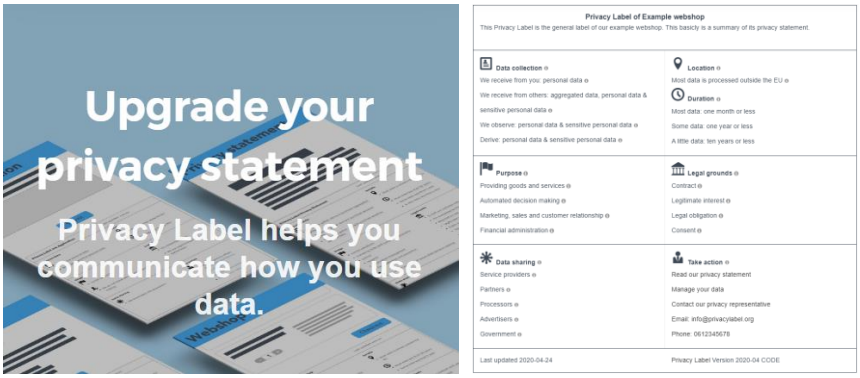
[15] Consumers' Association, 9 May 2018, 'Majority of people keeps account statements for at least 5 years', https://www.consumentenbond.nl/betaalrekening/meerderheid-bewaart-rekeningafschriften-ten-minste-5-jaar

Solution: Machine-readable privacy label

The GDPR offers an opportunity for more intelligible information in Article 12(7). This article makes clear that the information to be provided to data subjects pursuant to the ensuing Articles 13 and 14 may also come in the form of standardised icons. Logically, there may also be similar, communicatively simple and easily accessible alternatives. Where the icons are presented electronically, they shall be machine-readable, so privacy statements can be interpreted by software, which in turn may create new services.

An example of how information may be presented, is offered by the Privacy Label (www.privacylabel.org). Through this label it is possible to make clear the most important elements of the processing of personal data. In addition, this information is machine-readable and therefore the information becomes suitable for further use.[16]

We would like to emphasise that this is an existing piece of technology that can be applied directly. Similar technologies probably exist.



Figuur 4: Screenshot and example of the Privacy Label

[16] https://www.privacylabel.org/learn/

Solution: Good practice of the Dutch National Forum on the Payment System

Another example of providing meaningful information and complaice to articles 12, 13 and 14 GDPR on the processing of personal data is supported by the Dutch National Forum on the Payment System (Maatschappelijk Overleg Betalingsverkeer (MOB)).[17] In its meeting of 26 May 2020, the Forum approved the 'good practice account information services' in order to obtain transparency about account information services under PSD2.[18] To promote this, it has drawn up a good practice that includes seven questions for account information service providers to be answered concisely and comprehensibly before data subjects authorise providers to access their account. In their statement:

Offering service in the Netherlands? Take good notice of these good practices

Good practice for account information services in the Netherlands

At its meeting of 26 May 2020, the National Forum on the Payment System (NFPS) endorsed the good practice document for account information service provision in the Netherlands. The NFPS previously observed that consumers and firms both need transparency about account information services provided under PSD2. To help account information service providers provide such transparency, the NFPS has drawn up a good practice list consisting of seven questions. Service providers can answer these questions concisely and clearly before asking the account holder's consent to access his or her account. We have discussed competition and privacy aspects of the good practices with the Authority for Consumers & Markets (Autoriteit Consument & Markt –

[17] https://www.dnb.nl/en/inclusive-society/national-forum-on-the-payment-system/

[18] For the press statement including attachments, see the website of the DNB: https://www.dnb.nl/en/actueel/dnb/news-2020/results-from-the-nfps-meeting-of-26-may-2020/; for the documents, follow the links in the press statement or follow these links: https://www.dnb.nl/media/knwdp5ia/good-practise-for-account-information-services-in-the-netherlands.docx and https://www.dnb.nl/media/j44nwlih/explanatory-notes-to-the-good-practise-account-information-services-in-the-netherlands.docx

ACM) and the Dutch Data Protection Authority (Autoriteit Persoonsgegevens – Dutch DPA).

(…)

Proposed good practice
The NFPS secretariat proposes that the members of the NFPS can ask licensed account information service providers in the Netherlands19 to refer users (i.e. consumers or small firms) to their answers to the seven questions before requesting their consent for access to a payment account in order to provide the account information service offered.

Account information service providers will be asked to formulate their answers concisely and in plain Dutch (language proficiency level B1), providing examples and illustrative details, while not exceeding two A4 pages. In addition, the questions have been made even more specific.

The questions must be answered separately for each specific service, as service providers may well offer separate services with specific characteristics.

It is important to realise that these questions were drawn up by consumers. They overlap with and come in addition to the information requirements of Articles 13 and 14 GDPR but are more succinct and more focused on the information needs of consumers. These are the questions:

1. Who is requesting access to my account information? Which rules apply to the service?
2. What service does <*name of service provider*> provide for which it needs my information?
3. What account data will <*name of service provider*> be using?
4. What else will <*name of service provider*> be using the data for?
5. What data will be shared with third parties, and why?

[19] They can be licensed payment institutions, electronic money institutions, banks and registered account information service providers.

6. How can I withdraw my consent once I have given it?
7. Where can I find more information?

Our suggestion is to adopt the best practices of the Dutch National Forum on the Payment System as an approach to meet consumers' information needs. More information can be found on the webpage as mentioned in the footnote on the previous page.

Solution: Keeping in mind several focus points

Inform on data storing after ending of contract

When informing consumers about the period for which their personal data will be stored, this information should logically also include what service providers do with data as soon as a contract is terminated, consent concerning the data transfer to an AISP is not renewed, or a given consent under Article 94(2 PSD2) is revoked within 90 days.

Inform consumers in a timely manner

Service providers have to inform data subjects in a timely manner. The GDPR adheres to providing information before processing begins. Because the PSD2 assumes a contractual relationship, a person who considers entering into a contract will have to first have information in order to make this assessment. In light of this, it is striking that information about a particular service cannot always be found. Information about the services themselves is often available only after a person has purchased a service or has downloaded an app from the Google Play Store or Apple's App Store (iOS). Information with regard to specific services should be placed on a generally accessible website where it is complementary to the information that is provided to consumers when they are in the process of purchasing a service.

Privacy-related services must be at the same level of commercial services

The GDPR provides the framework for the processing of personal data and controllers have to adapt their own organisations to a large number of legal provisions. Organisations must interpret the GDPR in such a way as to guarantee the fundamental rights and freedoms of data subjects. Privacy-related services must be at a comparable level to that of other

services, in order to make sure consumers are able to exercise their rights throughout the whole spectrum of services. Terminating a contract should be as simple as entering into one.

We would like to emphasise that communication and communication technologies are constantly evolving. Two examples of this are *microtargeting* and *neuromarketing*. The way in which information is provided and communicated transparently should be appropriate and in line with the current state of technology, as laid out in the data protection policies of Articles 24 and 32 GDPR. With best practices for information security in place,[20] there is no less a need to also establish best practices in the field of business-to-consumer communications. As AISPs use modern communication technologies to bring all sorts of services to the attention of consumers, they will need to pay closer attention to providing accurate information and the way in which they inform consumers. In other words, the information they provide with regard to privacy and data protection as demanded by the GDPR should be as good and convincing as their sales information.

Act on your customers' needs and exceed their expectations

The power of revoking consent

It is important to provide mechanisms to data subjects to allow them to control the processing of their personal data. Likewise, they should be enabled to update or even retract their personal information. AISPs should ask for consent (and allow it to be withdrawn) whenever relevant. They should also offer data subjects a meaningful choice, allowing them for example to use a website with limited functionality if they do not consent to share their personal details.

[20] 'What is ‘‘state of the art’ in IT security?' ENISA and TeleTrusT - IT Security Association Germany have, 7 February 2019 (https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/)

With regard to the provision of data by consumers, consent is an important safeguard within the PSD2. Consent must be reconfirmed every 90 days. If consent is not renewed, no data may be processed and the account of the data subject becomes inactive. Logic dictates that the basis for processing comes to an end following the active withdrawal of consent. The data subject will have to be offered to delete their data in order to do justice to Article 5(1)(3) and (17) GDPR. The retention of data after consent has been revoked means the continuation of processing of said data and thus constitutes a violation of GDPR principles.

When a person withdraws their consent within 90 days, they make a an 'unambiguous choice'. The withdrawal of consent is currently without consequences since no action is required (although we dispute that) so often the processing of personal data continues. It would be expected that one of the consequences of consent withdrawal by data subjects is that they are given the opportunity to submit a request for data erasure on the grounds of Article 17 GDPR, which should be complied with immediately. Incidentally, the processing party itself would have to decide to do so, as with the withdrawal of consent the basis for processing disappears.

Don't allow sub optimal solutions

The processing of special categories of personal data is in principle prohibited. In all likelihood, the only ground for exception to this rule is explicit consent, as laid out in Article 9(2a GDPR). The EDPB points out that it should be possible to use a service without sharing categories of sensitive personal data. This is similar to offering different services, where withholding consent should not have a negative effect on the use of the service.

In the case of sensitive personal data, however, the suboptimal provision of services is likely to happen. Consent for the use of sensitive personal data can be seen in a number of forms: (a) sensitive personal data are not identified. (b) personal data are seen as part of the entire data set, so those who wish to protect their sensitive personal data will have to refrain from using the service altogether. This will not allow the person to enjoy the opportunities that the legislator intends to give. Many consumers will still give their consent, while they would make a different

choice in case they would be given the opportunity to purchase a service without providing any sensitive personal data. As far as we are concerned, the handling of sensitive personal data falls all too frequently into the category 'take it or leave it', a course of affairs that the EDPB rejects in its guidelines.

An example of this practice can be found at an AISP which states the following in its privacy policy: "Please be aware that if you do not want us to process the data for the purposes set out above, we cannot provide our services to you." This party asks permission for six processing targets, and states it has a legitimate interest in 26 sub-targets.

Giving permission for the processing of sensitive personal data is based on the principle that consent must be given 'freely'.

Closing remarks

Sensitive personal data are only a very small part of the whole set of financial transaction data. It will be difficult to estimate what negative effects the processing of these sensitive personal data will have on data subjects. Regardless, there is no doubt in the mind of Privacy First that these data merit additional protection.

~~ End of document ~~