PRIVACY FIRST
your choice in a free society

Postbus 16799
1001 RG Amsterdam
Tel. 020 - 8100279

To	:	European Data Protection Board
Our ref.	:	SPF20200915
Date	:	16 september 2020
Topic	:	Feedback on Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR

1. Introduction

Honourable members of the European Data Protection Board,

This document contains Privacy First Foundation's response to the Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR - version 1.0, open for Public consultation under reference 06/2020. The Privacy First Foundation is a Dutch foundation registered as having a charitable status (ANBI).[1] It 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. Against this background we will discuss some of the issues in your draft guidelines.

The Privacy First Foundation has been concerned with financial privacy for years. Since 2017, we have been involved in the developments around PSD2 and have been concerned about the privacy of those involved from the very first moment. As an NGO that promotes civil rights and privacy protection, we focus on privacy concerns that arise around the 'account information service providers' ('AISP') and possibilities for further processing of personal data.

At the end of 2017, we thought that better information and transparency would be sufficient for those involved. The risks turned out to be greater and more fundamental. We then expressed our concerns to a wider audience during the broadcast on Dutch television of AVROTROS Radar on Monday evening 7 January 2019.[2] Our concerns regarding the PSD2 are included in our PSD2 project. Through this project, we aim to contribute to making positive improvements to the PSD2 and its implementation in order to achieve better privacy protection. Our website PSD2meniet.nl contains information in Dutch and English about the PSD2 and provides an outline of both our concerns as well as our solutions, such as the Don't-PSD2-me-Registry.[3]

---

[1] Public Benefit Organisation (Dutch: *Algemeen Nut Beogende Instelling*, ANBI)
[2] See: https://privacyfirst.nl/acties-3/psd2meniet-nl/item/1137-privacy-first-eist-psd2-me-niet-register.html and https://radar.avrotros.nl/uitzendingen/gemist/item/wat-betekent-de-nieuwe-betaalrichtlijn-psd2-voor-jou/ (Dutch)
[3] https://psd2meniet.nl/en/

Although the PSD2 and GDPR provide safeguards to protect the fundamental freedoms and rights of data subjects, the effective protection of data subjects lies in the proper implementation and interpretation of the GDPR by the account information service providers. Your guidelines therefore play a key role.

We would like to compliment you on the comprehensive document that provides a lot of information on how account service providers should deal with their services under the PSD2. A number of concepts and principles are well elaborated so that under the PSD2 service providers cannot hide behind a poor interpretation of the PSD.

Nevertheless, we would like to make several general suggestions and bring to your attention a number of specific areas for improvement that may contribute to better guidelines.

2. Outline of the risks

Significant differences between PSD2 and GDPR levels of protection

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 will particularly apply to AISPs that wish to provide additional services or further process personal data. In this case safeguards only derive from the GDPR. We want to caution against paper tigers and call attention to enforcing and monitoring privacy by design, thereby mitigating or excluding from the outset risks to fundamental rights and freedoms of data subjects.

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 in a relatively lower sanction, i.e. a fine of up to €20M or 4% of the worldwide turnover.[4] In practice, the fines will probably be even lower, as evidenced by the fine decision of the Dutch Data Protection Authority.[5] Apart from that, the regulators' supervision is reactive and not part of an annual review of a licence.

Full control over personal data must be the objective

In point 1 of your document you state that "certain questions and concerns in respect of the **need** that the data subjects remain **in full control** of their personal data [emphasis by us]." 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 this goal can be achieved to the benefit of the data subject. It may take a far-reaching form of Personal Data Management (PDM) to give a person full control, up to the point where the data subject is no longer dependent on the AISP.

There are already good technologies and applications that allow a person to process their data by use of a smartphone. For example, we point to initiatives such as 'the Financial

[4] Article 83 GDPR
[5] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan

Passport' (Financial Passport Foundation[6]) or the 'rental passport' (Qii[7]). Access to a person's own data should be made possible by the PSD2 as a matter of principle. Article 20 GDPR offers the possibility of data portability. This right of a data subject is hindered by the PSD2. From this point of view, PSD2 legislation can in fact even be called partially unnecessary. The risks to the interests and rights of data subjects should therefore be seen in comparison with the possibility of sharing information *without* a third party.

Data subjects are hardly able to exercise their rights, partly due to profile enrichment

Once a data subject's data is 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 regardless. In coalition with others, Privacy First is raising this issue in a class action lawsuit under Article 80 GDPR against two major technology firms.[8] With PSD2, profile enrichment will be even easier and will have a greater impact than the separate data that are being collected now.

PSD2 may pose risks for debt assistance

An area in which insight into financial matters is important, is debt assistance. In the Netherlands, at least 38 (online) accounting packages[9] and at least 18 online housekeeping manuals[10] are offered to individuals. Many of these parties will want to make use of a PSD2 connection. As long as the data are used for the primary AISP services, the risk of unlawful processing is limited. However, the data make it attractive to offer additional services. Experience shows that parties use third party services to create profiling, online markets to make offers and risk and credit ratings to set up risk profiles. For people in a vulnerable position as a result of debt problems, the use of AISPs will hardly be a free choice. The same applies to additional services offered. Our contention is therefore, 'once given means given once and for all'. It is important that risks are eliminated *before* data are shared, and that those concerned are afforded maximum protection.

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

The GDPR provides the framework for the processing of personal data. A large number of legal provisions have to be adapted by the controller to his own organisation. The organisation 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 avoid that exercising one’s rights becomes more difficult compared to other services. Terminating a contract should be as simple as entering into one.

---

[6] https://financieelpaspoort.nl/
[7] https://qii.nl/
[8] https://www.privacyfirst.eu/focus-areas/online-privacy/689-the-privacy-collective-takes-oracle-and-salesforce-to-court.html
[9] https://www.boekhoudeninexcel.nl/verdien-200-euro-per-jaar-met-de-besparingschecker/
[10] Consumers' Association (Consumentenbond), 31 March 2020, 'Digital household books', https://www.consumentenbond.nl/budgetteren/digitale-huishoudboekjes

3. General comments

In accordance with Article 108 PSD2, the European Commission shall evaluate the Directive as from 13 January 2021. We express the wish that elements of the guidelines will be enshrined in law where possible, for example by including a reference to this opinion or inclusion of provisions in the explanatory recitals to articles.

I. ***Suggestion***: Inform the European Commission about these Guidelines and let them be part of the PSD2 evaluation together with insights you gain during the consultation.

In our opinion, the greatest risks to the privacy of data subjects arise when an AISP wants to start offering additional services, or when a service provider wants to start using AISP services in collaboration with a third party. This will involve new of extending of services and/or further processing of personal data. Because there is already a relationship, in these cases the provider has more opportunities to influence the behaviour of the consumer and thus the threshold and initial guarantees will be lower, increasing existing risks.

The possibility of further processing is described in section 2.3, points 20 to 24. This possibility is therefore the primary focus of our efforts and this evaluation. At that time, 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 a data subject.

II. ***Suggestion***: Underline that controllers and processors should explain the GDPR in favour of data subjects. Deadlines concerning the rights of data subjects (Article 15 and continued GDPR) are the longest possible deadlines that are used only in exceptional cases.
III. ***Suggestion***: Emphasise that the privacy-related elements of both the PSD2 and the GDPR should be explained and that a data subject has full control over their personal data. This means that any delay in exercising rights, inadequate communication or tactics that cause consumers to make choices that they regret at a later stage, make the processing of personal data unlawful.
IV. ***Suggestion***: indicate where the main risks arise for data subjects or refer to a DPIA carried out in the context of the PSD2 in which these risks are identified, if any is carried out,

The Committee will have to consider that at its core the PSD2 creates new risks. A central problem of the PSD2's new possibilities offered by PSD2 lies in the use of a third party such as an AISP. For example, if a person has three bank accounts and wants to have these in a

single overview, they will have to use the services of a third party, the AISP.[11] This puts the third party, the AISP, between the communication between a consumer and a bank. The law should allow a person to have access to all their data in a different environment from that of the bank in accordance with Article 67(1), but without involving a third party such as an AISP. Although the PSD2 creates a new possibility, it also creates a new risk by obliging this third party.

V. ***Suggestion***: In the process of drawing up guidelines, keep in mind the alternative of allowing a consumer access to their payment details without having to involve a third party such as an AISP, and continue this line of reasoning from this point on.

Consumers cannot limit the amount of bank data shared after they give their consent. Even if a financial services provider does not need these data, all data are shared after consent has been given. This is contrary to the principle of data minimisation under the GDPR. Your guidelines can be strengthened by providing a few examples. Examples include restrictions on the duration for which data are shared, distinguishing between income and expenses and excluding certain values before they are processed further.

VI. ***Suggestion***: Use examples of applications to illustrate processing boundaries.

4. Transparency and information

Chapter 6.4 of the draft guidelines deals with transparency and accountability. Currently, consumers are not properly and fairly informed. Much of the provided information is often difficult to read. This is an bad thing, not least because a lot of value is attached to their explicit consent. But how much value does consent have if a consumer cannot sufficiently assess the consequences of giving consent?

The call for clear information is not limited to this financial information. A consumer who wants to use an AISP shares their data with a third party. It involves as much information as is available from the payment service provider, which essentially is a lot. 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 data of, on average, the past seven years.[12] Some banks show details from only the past two years while newer banks do not even have a maximum term and can eventually contain a lifetime of transactions.

By using services for further processing 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

[11] See recital 28 PSD2 on which this example is based.
[12] Consumers' Association, 9 May 2018, 'Majority keeps account statements for at least 5 years', https://www.consumentenbond.nl/betaalrekening/meerderheid-bewaart-rekeningafschriften-ten-minste-5-jaar

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.

Instead of the EDBP limits its position on providing the legally required information, it is recommended that the EDPB draws the attention of providers to the importance and usefulness of information. An understanding of the processing, risks and insight into the nature and scope of the processing is important in this respect.

In points 8 and 10, the voluntariness of a person to use a service is mentioned. It is expected that financial services providers will specify whether or not their services use a link to PSD2 for credit assessments. This specification should only be allowed if a provider provides sufficient safeguards in the form of preventing profiling, not adding datasets to other information of the person and strict data minimisation. Even under these conditions, the dividing line between 'enticement', 'gentle coercion' and 'involuntariness' 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.

When writing its guidelines in support of supervisory tasks, the EDPB will have to realise that privacy statements are too long and difficult to fathom. In our own research into the privacy statements of Yolt, Spiir and Google Pay, we found that the number of pages that make up the privacy statements of these companies was 8, 13 and 4, respectively, with Google Pay linking its privacy terms and conditions to its general terms and conditions totalling 31 pages. The privacy statements examined all had different designs, structures and layouts. This does not help consumers in assessing the information.

Article 12 GDPR states that information should be provided in a concise, transparent, comprehensible and easily accessible form and in clear and simple language. This information was omitted in de guidelines. Practice shows that information is often not provided in accordance with these standards.

VII. ***Suggestion***: Confirm that information must be provided in accordance with the requirements laid down in Article 12 GDPR.

The EDPB could draw attention to instruments that make the obligation to provide information accessible. The GDPR offers an opportunity for this in Article 12(7). This article makes clear that the information to be provided in Articles 13 and 14 GDPR may also come in the form of icons. Logically, these could also be similar, communicatively simple and easily accessible alternatives. The EDBP could make an effort to draw attention to this article. It is

mentioned that icons are machine readable. When icons are machine readable, they can be interpreted by software which may create new services.

VIII. ***Suggestion***: Emphasize that payment service providers should provide information simply. Appoint the option of Article 12(7 GDPR) mentioning the possibility of icons or comparable alternatives.

IX. ***Suggestion***: Emphasise the possibility mentioned next to the icons of Article 12(7), namely that information is machine readable. This creates the possibility of comparability of information between providers.

We would like to emphasise that communication and communication technologies are also evolving. An example of this is *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 is the case with data protection policy as set out in Articles 24 and 32 GDPR. Similar to the best practices for information security,[13] this may also be declared applicable to communication. We note that modern communication technologies are used to bring the services to the attention and put these in a favourable position. In order to achieve a balance between technologies and information, you will need to pay attention to this in your guidelines.

An example of how information may be presented, is offered by the Privacy Label. 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. [14] We would like to emphasise that this is an existing technique that can be applied directly. Probably more of these techniques exist.

X. ***Suggestion***: Be aware that there are tools for presenting information in an accessible way and that these should be seen as 'state of the art' in the field of communication.

XI. ***Suggestion***: Emphasise that means of communication around the rights and freedoms of data subjects should be balanced with means of communication used to promote commercial services. Stress that providers must strike a fair balance in this respect.

XII. ***Suggestion***: Present the method of the Privacy Label as an example of an approach to meet the GDPR's information obligations in an accessible, concise and simple manner.

Another example to provide meaningful information on the processing of personal data is supported by the Dutch National Forum on the Payment System (Maatschappelijk overleg betalingsverkeer (MOB)).[15] In its meeting of 26 May 2020, the Forum approved the 'good

[13] 'What is "state of the art" in IT security?' ENISA and TeleTrusT - IT Security Association Germany have, February 07, 2019 (https://www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/)
[14] https://www.privacylabel.org/learn/
[15] https://www.dnb.nl/en/payments/other-tasks/national-forum-on-the-payment-system/index.jsp

practice account information services' in order to obtain transparency about account information services under PSD2.[16] To promote this, the MOB has drawn up a good practice that includes just seven questions to account information service providers to be answered concisely and comprehensibly before the user authorises the provider to access their account. It is important to realise that these questions were drawn up by consumers. They overlap with the information requirements of Articles 13 and 14 GDPR but are more succinct and more focused on the information needs of the consumer. These questions come in addition to the information obligations. The questions are:

1. Who is asking for 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?
6. How can I withdraw my consent once I have given it?
7. Where can I find more information?

XIII. ***Suggestion***: adopt the best practices of the Dutch National Forum on the Payment System as an example of an approach to meet consumers' information needs.

In order to improve information and transparency, you can refer to other themes in financial services. Information on financial services is difficult to grasp and often does not achieve its intended purpose. In July 2019, Dr. C. de Jager obtained her PhD with a thesis in which she states that financial leaflets for clients are often difficult to understand, among other things, due to technical language and therefore fail to achieve their purpose.[17] Meanwhile, a European Information Document, the Key Information Document (KID) pursuant to Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail investment products and insurance-based investment products (PRIIPs), is now being used.

In response to questions from the Dutch Parliament, the Minister stated the usefulness of good information (in relation to the KID): "In order to increase the readability of the KID, the KID must be a stand-alone document and should not contain references to marketing material. In order to further increase the legibility of the KID, the KID uses some of the prescribed texts or figures that are required to be included in the document. Finally, unlike the financial information leaflet, the KID must be provided to the consumer before that consumer is bound by an agreement or offer relating to the product. The aim is to give the

[16] For the press statement including attachments, see the website of the DNB: https://www.dnb.nl/en/news/news-and-archive/nieuws-2020/dnb388945.jsp
[17] Jager, C. de (2018), 'Consumer protection through information? (Thesis RUG)

consumer time to gain a better understanding of the risks, costs and the intended return." The European Commission will evaluate the KID and see if it contributes to a better understanding of the financial service.

XIV. ***Suggestion***: recommend that transparency and information be directed to stakeholders in similar ways as is customary on other issues in the financial sector, for example with the European Information Document, the Key Information Document.

In point 74 the EDPB indicates that the data subject should be informed in particular about the period in which the personal data will be stored. This information should logically also include how the provider handles data as soon as a contract is terminated, or consent under the data transfer to an AISP is not renewed, or a given consent under Article 94(2 PSD2) is revoked within 90 days.

XV. ***Suggestion***: Note in point 74 that a provider must indicate how it handles personal data once a contract is terminated, or consent under the data transfer to an AISP is not renewed, or a given consent under Article 94(2) PSD2 is revoked within 90 days.

XVI. ***Suggestion***: Highlight the moment in time in point 75 in the part that reads: ‘‘that the information must take place no later than the time of 'the first communication'.’’ Logically, this takes place before a contract is concluded.

Your Guidelines can contribute to improved information by making a statement on the timing of information delivery. 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 this light, it is striking that information about a particular service cannot always be found. Information about the services themselves is often only available once a person has purchased a service or has downloaded an app from Google Play or Apple’s App Store (iOS). The EDPB could advise to place information about such specific services also on a generally accessible website and to make this information complementary to the information that is provided to consumers when they are in the process of purchasing a service.

XVII. ***Suggestion***: Point out that the provision of information in the context of the obligation to provide information and transparency under Article 12 of GDPR should happen in a timely fashion. This means during the process in which a person decides whether or not to give their consent. If a person is informed too late, supervisors will have to consider the consent as unlawful.

5. Explicit consent

We will here discuss chapter 3 of your document which relates to explicit consent. As in your letter of 2018, you indicate that explicit consent under the PSD2, given in Article 94(2), should be seen in the contractual context. You conclude at point 43 that explicit consent under the PSD2 is not the same as (explicit) consent under the GDPR. The difference is that consent under the GDPR provides a basis under Article 6 GDPR and explicit consent under the PSD2 provides an additional contractual requirement.

What is not clear is whether the consent referred to in the PSD2 must meet all the requirements and criteria that apply to consent under the GDPR. In addition, you mention a number of elements that consent under the PSD2 must meet, but fail to make clear whether they fully meet the requirements of consent under the GDPR, or where they differ.

XVIII. ***Suggestion***: Confirm or clarify similarities and differences between the requirements for consent under the GDPR and the PSD2.

Consent within the GDPR is 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 GDPR uses the term 'informed' as part of valid consent. This is generally misinterpreted as simply providing the data subject with the legally required information, thereby complying with the controller's responsibility. The intended effect of the GDPR is that a person can make an informed choice about the processing of their personal data on the basis of information. In the case of PSD2, this principle is undermined. Meanwhile, there is no longer such thing as an informed data subject because the scope of the consent given can no longer be overseen. The effect will be that, although a person knows 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.

When advising regulators and providers of PSD2 services, it is worth remembering that providing information does not automatically mean that a person can grasp the scope and capabilities of the provider. Especially once an AISP carries out further processing or, or commissions a third party to do so, it will be difficult for a data subject to assess the impact of sharing a full financial profile.

XIX. ***Suggestion***: Better explain what the purpose of informed consent should be, what a data subject can expect and how a provider can check whether a data subject is aware of what they have consented to.

Consent is an important safeguard within the PSD2 with regard to the provision of data by consumers. It is not clear whether the legislator sees the explicit consent as a guarantee from a privacy protection point of view since it must be seen in the contractual sphere.

However, it is presented as privacy protection safeguard by the Dutch Central Bank and Dutch banks in their information to consumers.

In the draft guidelines, the EDPB does not comment on the withdrawal of consent. Consent must be reconfirmed every 90 days. If a person does not renew their consent, no data may be processed, and the account becomes inactive. Logical 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 and leads to 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 now without consequences, while the processing of personal data continues. It would be to be expected that the consequences of consent would be that, as soon as a person withdraws their consent, they are given the opportunity to immediately submit a request for data erasure on the grounds of Article 17 of the GDPR, which should then 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.

The direct consequence of withdrawing someone's consent, i.e. data erasure, is not dealt with in the guidelines. For us it is self-evident that it is at least desirable for the data subject to be offered the possibility to request data erasure.

XX. ***Suggestion***: Elaborate further what is expected of a provider once a data subject withdraws their consent under Article 94(2 GDPR). Also address the consequences for data that are still being retained and are part of internal operations, profiles and statistics. Specify the rights a person has and which should be 'activated' once consent is revoked, in particular Article 17 GDPR (data erasing).

In point 31 you refer to the EDPB guidelines 05/2020 which state that signing a written declaration is a good way of giving consent. In the case of PSD2, it would be advisable to conform to authentication forms known in the banking world, such as agreeing via a two-factor authentication or through the portal of the relevant ASPSP.

XXI. ***Suggestion***: In addition to a written statement, allude to digital means by which a given consent can be demonstrated according to Article 7 GDPR.

Unfortunately, point 34 fails to make clear how the exception of Article 33 PSD2 works. We point out that the explicit consent of Article 94(2 PSD2) has often been mentioned as a guarantee. Article 33 PSD2 excludes AISPs from this consent, but not the actual provision of services. It is not clear why this is and what the material effect of this is. This apparently erodes the guarantee of Article 94 paragraph 2 PSD2. The last part of point 38, in conjunction with point 39, does not provide clarity on the connection. With regard to your point on the 'central consideration that the data subject must be able to determine in

advance the extent and consequences of the processing and that they should not be taken by surprise at a later point about the ways in which their personal data have been used' we refer to our input on transparency and information.

XXII. ***Suggestion***: clarify the relationship between point 34 of the draft guidelines in relation to the exception of Article 33 PSD2 to Article 94(2).

With regard to point 30, the processing of special categories of personal data is in principle prohibited. There are exceptions where the explicit consent of Article 9(2a GDPR) is in all likelihood the only ground for exception. This point relates to points 40 and 42. You note 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, this is, however, 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 'whole', so those who wish to protect their sensitive personal data will have to refrain from using the entire service. This will not allow the person to enjoy the opportunities that the legislator intends to give. Many people will still give their consent, while they would make a different choice were they 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 easily falls into the category 'take it or leave it', as you reject in point 18.

An example of this practice can be found at an AISP[18] who 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, that we cannot deliver you our services." This party asks permission for six processing targets, as well as a legitimate interest which includes 26 sub-targets.

Giving permission for the processing of sensitive personal data is based on the principle that consent must be given 'freely'. Sensitive personal data are only a very small part of the whole of transaction data. It will be difficult to estimate what negative effects the processing of this personal data will have on a person. However, the protection of sensitive personal data concerns not only the private data in question, but also in the principle that these data deserve additional protection.

XXIII. ***Suggestion***: In paragraphs 30 and 42, stress that a person who wishes to give consent under Article 94(2 PSD2) but wishes to withhold consent for sensitive personal data should still be able to use the service provided. Especially in the case of further processing as referred to in Article 5(1)(b) of GDPR.

[18] www.yolt.com/privacy, 1 September 2020

6. Processing of silent third-party data

A consumer's bank details also contain the details of someone else's account, which is the 'silent third party'. This person does not know that their data are being shared and cannot prevent it. Because the transaction data will be analysed much more widely via Big Data and data analyses than before the entry into force of PSD2, there are major risks of privacy violations. Your letter of June 2018 to the European Parliament seems a legal solution to a fundamental problem. We are therefore pleased that the current draft guidelines deal with this subject. However, they do not address the fundamental problem quite sufficiently.

As with the special categories of personal data, the starting point is the ability to filter data from silent parties. Principally, a person who is part of a transaction will have to be assured that their data is not included in processing operations in which they are not involved and in relation to which they cannot exercise their rights. Providers of AISP services claim a legitimate interest in processing the whole transaction. Nevertheless, the inequality of rights leads to undesirable effects. It should be recommended to providers of PSD2 services to provide the possibility of *not processing* data from silent parties. It should be clear that the processing is due to the nature of a transaction involving two parties and the processing of data from the silent party is a hard-to-avoid bycatch. This does not exempt processing parties from taking measures to limit the processing immediately upon receipt of the personal data.

Data subjects should have the right, invoking Article 18 GDPR, to object in advance to the processing of their data by PSD2 services providers. Providers may take general measures or allow individuals to exclude their account number from certain services. Stakeholders could inform their bank of their preference or, to this end, make use of a Personal Data Management (PDM) application.

This is mainly about the further processing of the data. Due to the large amounts of data they process, credit rating providers – companies specialising in profiling or risk assessments – to process data from silent persons and ultimately connect these data to the profile of this silent person.

In paragraph 4.1, points 48 and 49, the Committee appears to state that personal data of the silent party may not be processed further. However, the paragraph still seems to give room for this. The Committee could state more clearly that the data of silent parties may not be processed further, apart from a legal obligation. AISP's will have to take measures to do so.

XXIV. ***Suggestion***: Describe more clearly that the further processing of data from a silent party is not permitted, in particular with regard to profiling or constructing profiles, enriching existing data and developing network profiles.

XXV. ***Suggestion***: Point out to providers that they must take technical and organisational measures to prevent further processing on the grounds of a legitimate interest.

7. Processing of special categories of personal data under the PSD2

Bank data contain 'special categories of personal data' that can only be processed under strict conditions. A membership payment to a trade union, political party or organisation that reveals sexual preference should be seen as particularly sensitive personal data. Transactions with healthcare providers and pharmacies should also be regarded as sensitive personal data. At present, it is not possible to filter these data and they are provided to parties that are not permitted to process these data. As far as Privacy First is concerned, there is no reason *not* to offer consumers the ability to limit the data sharing. There is a solution that makes it possible to filter these data, and which should be used as a starting point for further monitoring. We will elaborate on this on the next page.

Privacy First welcomes the description of point 51. The role of sensitive personal data and the fact that they can be derived from transactions seems to have been underexposed for a long time. We are equally pleased with points 56 and 57. We here refer to other sections in these recommendations about consent. We wonder if the intended quality of consent is achieved within PSD2. For special categories of personal data, this is particularly risky.

In point 52, you indicate that parties must investigate to prevent the processing of certain data points. One possibility you mention is to carry out a DPIA. Although we do not dispute the fact that a DPIA can identify sensitive personal data in accordance with Article 35 of the GDPR, this instrument is insufficient for the purpose. Both the Committee and the European Commission can play a better role here. The crux of the matter is that a service provider may not know and has no incentive to investigate in which cases sensitive personal data exist. When processing this transaction data, the service provider may not realise or want to realise that the transaction reveals sensitive personal data. There is also a risk that a provider will underestimate the risk of infringement of a data subject's rights and freedoms, for example because it involves a very small number of transactions in relation to the overall number of transactions.

XXVI. ***Suggestion***: Emphasise that if a DPIA shows that special categories of personal data are being processed, this is already enough ground to take measures.

At PSD2meniet.nl/en it has been elaborated how a PSD2 service provider can verify that there is a special category of personal data. Sensitive personal data can often be linked to organisations one-on-one. These organisation can easily be found.

Within Europe, organisations are categorised according to the European NACE Rev. 2.'[19] NACE Rev. 2 contains a statistical classification of economic activities in the European Community. By connecting organisations to categories of sensitive personal data, it is easy to identify which organisations are involved. Organisations within these categories can subsequently include the relevant account number in the registry. If a separate account

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

exists for membership fee or membership then only that number needs to be recorded. [20] PSD2 service providers can use these account numbers to exclude special categories of personal data from processing. We believe that in any case this concerns organisations within the following categories:

Political views

- 9492 Political organisations

Religious or philosophical beliefs

- 94911 Religious organisations
- 94919 Experiencing, deepening and/or spreading a philosophy of life not being a religion

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 the mentally disabled and psychiatric clients
    - 873 Homes and day care homes for the non-intellectually disabled and care homes
    - 879 Youth care and social care with overnight accommodation
- 4773 Pharmacies

Two categories organisations are less clear although they can be identified easily.

Race or ethnicity

- To be deduced from behaviour such as send/recipient of amounts, payments to certain organisations

Data relating to a person's sexual behaviour or sexual orientation

- To be deduced from behaviour such as send/recipient of amounts, payments to certain organisations such as those representing the LHBTI+ community

The European Commission or the Committee may take the initiative to set up an independent register of account numbers, in which a transaction by or to the account holder can be regarded as sensitive personal data.

[20] A much heard argument against recording is that a transaction does not necessarily have to express f.e. a political or sexual preference. A donation to a patients organisation doesn't mean the person has this particular disease. We see such arguments mainly as a method of not having to take action. We would point out that organisations that draw up profiles do record and interpret this information and can thus influence a person involved.

Within our project PSD2meniet.nl we have started with designing and establishing such a register which demonstrates this can effectively be realised.[21] This shows that it is possible to make a provision as outlined in point 57: it prevents the inclusion of certain data points and provides a technical possibility to exclude special categories of personal data.

At a minimum, this register should include a provision for political parties. A conclusive overview of political parties can be deduced from the political parties registered for elections. We like to point out that the current protection provided under Article 9 GDPR is likely insufficient to safeguard the objectives of the International Covenant on Civil and Political Rights.

XXVII. ***Suggestion***: Specify that PSD2 providers should develop a possibility to exclude certain categories of sensitive personal data from further processing of personal data. Please assume that it is already possible to identify relevant organisations, as we show above.

XXVIII. ***Suggestion***: At least draw up a list of account numbers used for contributions, gifts or donations to political parties

XXIX. ***Suggestion***: Adopt and expand the Don't-PSD2-me registry.

With regard to the processing of criminal data, we would like to point out a risk that we perceive within the Netherlands but may also apply to other countries. Transactions can be traced back to fines and may thus reveal criminal information. On the website of the Dutch Public Prosecutor's Office there are several violations and associated fines. Fines and other transactions are transferred to one of the 12 publicly disclosed account numbers of the Central Judicial Collection Agency.[22] A transaction to one of the numbers reveals a criminal data.[23]

This information cannot only be used as part of a profile, it can circumvent an existing, regulated practice. The GDPR and the Dutch 'GDPR Implementation Act' allow private parties to use criminal data under Article 10 of the GDPR. In Article 33(2), the GDPR Implementing Act states that criminal data may be processed by private parties in the assessment to make a decision or carry out an activity, and to prevent criminal offences against that party. A clear example of how this data is used are the so-called 'Black Lists'[24]. According to the Dutch Data Protection Authority (AP): "The purpose of a blacklist is to alert organisations against certain individuals. This allows organisations to assess whether they want to do business with those individuals. For example, whether they want to let such individuals into their

[21] https://psd2meniet.nl/gezocht-rekeningnummer-voor-het-register/
[22] https://www.cjib.nl/rekeningnummer
[23] Even in case of more serious offences and crimes, fines provide a great deal of information. From the site '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 addition, for a large number of offences you will receive a criminal record. The 'Besluit justitiële en strafvorderlijke gegevens' (https://wetten.overheid.nl/BWBR0016544/2018-01-01/#Hoofdstuk2_Afdeling1_Artikel4) lists which offences are in any case included in the judicial documentation (one's criminal record).
[24] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/register-zwarte-lijsten

shop or let them stay in their hotel. A black list often contains criminal data or data about undesirable behaviour."

One cannot simply set up a blacklist. The AP offers an 'GDPR Manual Protocol Blacklist'[25] with blacklist requirements. A blacklist must comply with formal requirements, general information on processing such as the need for processing, information on the inclusion of blacklisted data subjects, guarantees for processing such as security safeguards for processing.

With PSD2 there is a risk that a person's criminal profile can be deduced on the basis of certain transactions. With these financial data in combination with public information a simple profile can be created. This can replace 'blacklists' and thereby circumvent the safeguards of the protection of fundamental rights and freedoms of the person concerned.

XXX. ***Suggestion***: Elaborate the different ways in which criminal data can be deduced from transaction data. Emphasise the safeguards and requirements as set out in Article 10 GDPR.

XXXI. ***Suggestion***: Examine whether transaction data obtained through a PSD2 service may be used for 'blacklisting' under Article 10 GDPR, bypassing important safeguards.

XXXII. ***Suggestion***: Emphasise that it should be possible to exclude criminal data when a data subject uses an AISP or wants to use data for further processing, as the risk of use for a criminal profile is too significant.

8. Data minimisation and privacy by design

In section 6.1 you clearly explain how providers should deal with data minimisation and privacy by design. At the moment, a major problem is that consumers cannot independently limit or filter the amount of bank data. Even if a financial services provider does not need certain data, all data is shared once permission is given. Subsequently, a consumer has no guarantee whatsoever that a service provider will carry out data minimisation.

We notice that providers often find it difficult to determine which data are necessary for processing and that they tend to come up with a broad interpretations of the rules.

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 a statement of income from the past two years is required. For many other services that are often conveniently placed under the heading 'innovation', the required data cannot even be determined, or the aim is to achieve 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 principles of data minimisation in jeopardy. The processing may be incorporated within the framework of the law, but the design of the processing may still be inaccurate.

[25] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/GDPR-handleiding_protocol_zwarte_lijst.pdf

XXXIII. ***Suggestion***: Bring to the fore that providers may be (are supposed to be) transparent about data minimisation and which pieces of information they receive is not used, even though they can be received under the law.

At the moment, the only party that determines when data minimisation occurs is the provider. In view of the position of the data subject and the fact that it is their data being processed, the Committee can draw the attention of the providers to the need for the data subject to be involved in determining which data they wish to share. Good opportunities are offered by different forms of Personal Data Management (PDM), which give a person control over what data are really required. Even if that means that certain services would be less effective.

You can also point to Article 35(9) GDPR in the guidelines, which explicitly refers to the involvement of (representatives of) those involved in the development of processing procedures and risk assessment.

XXXIV. ***Suggestion***: In point 63 you make a 'recommendation' while you could be more emphatic in your choice of words.

XXXV. ***Suggestion***: Identify the possibility of Article 35(9 GDPR) to involve data subjects or their representatives in a DPIA.

In point 62 you mention a number of data indicators that you suspect can be easily excluded. For example, the identity of the silent party, the transaction details and the IBAN of the silent party's bank account. We note that an AISP should also provide the possibility to exclude data within a category, such as the categories of special categories of personal data. Only then will a meaningful exception of data become possible.

XXXVI. ***Suggestion***: Highlight in point 62 that data minimisation may also involve filtering data within a category, such as categories of special categories of personal data.

9. Profiling

The chapter on profiling ignores the major risks associated with profiling. A lot of research has been carried out on profiling by credit scorers and data brokers. Closely related to this subject are the blacklists. In 2017, the weekly magazine *Groene Amsterdammer* featured an article titled 'You are on a blacklist'. [26] In 2020, questions about this have again been asked in the House of Representatives.[27] In September 2020 attention was given to profiling by de Dutch national television BNNVARA Kassa in their item ‘Commercial databases record data

[26] De Groene Amsterdammer, editie van 25 oktober 2017, nr. 43 over De schuldenindustrie 'U staat op een zwarte lijst'. https://www.groene.nl/artikel/u-staat-op-een-zwarte-lijst (2017).
[27] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?did=2020D34917&id=2020Z16169

on payment behaviour for creditworthiness'.[28] Other privacy NGOs such as Privacy International have paid extensive attention to profiling.[29] Profiling has also received attention in the academic world, with clear titles such as 'Profiling and targeting consumers in the Internet of Things provides new challenges for consumers'.[30]

Recital 28 of the PSD2 provides examples of services offered by AISPs: "Those services provide the payment service user with aggregated online information on one or more payment accounts held with one or more other payment service providers and accessed via online interfaces of the account servicing payment service provider. The payment service user is thus able to have an overall view of its financial situation immediately at any given moment. " This fragment gives a clear picture of an account information service. However, a sample of AISPs in the Payment Institutions Register[31] and a follow-up research on the service providers shows that it is often business-to-business providers and parties who can connect to credit ratings. These activities are based on profiling and are different from the considerations and terminology of the PSD2 and of recital 28.

In paragraph 6.5, points 79 and beyond safeguards around profiling are discussed. These guarantees are of value only if a data subject can retrieve or destroy their data from processing parties. It is therefore about removing data which are part of profiles and the updated profile. The profile or rating can have an huge impact on a person.

XXXVII. ***Suggestion***: Be more specific about the risks of profiling

XXXVIII. ***Suggestion***: Emphasise that people can suffer from long-lasting consequences as a result of profiling. Stress that parties must comply with their information obligations.

XXXIX. ***Suggestion***: Highlight that when a data subject actively withdraws their consent or makes a request for the removal of their data, source data with which profiles are created should also be removed, and the custom profile coding should be adapted based on the changed data.

XL. ***Suggestion***: Give examples that do more justice to the practice of AISPs, which process more than is described in recital 28 PSD2.

[28] BNNVARA Kassa, 12 september 2020, 'Commerciële databoeren registreren gegevens betaalgedrag voor kredietwaardigheid', https://www.bnnvara.nl/kassa/artikelen/commercile-databoeren-registreren-gegevens-over-betaalgedrag-voor-kredietwaardigheid

[29] www.privacyinternational.org

[30] https://www.ivir.nl/publicaties/download/1747.pdf

[31] https://euclid.eba.europa.eu/register/pir/search

PRIVACY FIRST
your choice in a free society

10. Final comments

We wish you every success with the next version of the Guidelines. Naturally we are always available to elucidate our recommendations. Finally, we would once more like to refer to our website PSD2meniet.nl for additional information about our project and activities.

Kind regards,

Martijn van der Veen

Privacy First Foundation
PSD2 spokesperson

Vincent Böhre

Privacy First Foundation
Director