THIS DOCUMENT IS AN ENGLISH TRANSLATION OF THE INFORMATION PUBLISHED BY THE DUTCH PROTECTION AUTHORITY ON 18 OCTOBER 2018 IN RELATION TO THE INTERPLAY OF PSD2/GDPR. THIS IS A COURTESY TRANSLATION PROVIDED BY BIRD & BIRD LLP – THE FIRM TAKES NO RESPONSIBILITY FOR THIS COURTESY TRANSLATION. THE OFFICIAL DUTCH LANGUAGE VERSION IS AVAILABLE HERE: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/betaaldiensten#faq

The protection of consumer privacy is an important part of the new European law on payment services (PSD2). A requirement under PSD2 is that payment service providers may only gain access to personal data of consumers if they have obtained explicit consent. Thus, the consumer decides whether a payment service provider may have access to his or her bank account and payment behaviour. The Dutch Data Protection Authority (AP) has now clarified, by means of Q&A's, what this 'explicit consent' requires.

PSD2 stands for the second Payment Services Directive. It is a European directive on payment services. This directive regulates not only banks but also other parties offering new payment and account services (for example, a service that helps to keep track of individual bank accounts).

The protection of consumer privacy is an important part of PSD2, because payment details are sensitive financial personal data. The legislation on the implementation of the directive is now handled by the senate.

Requirements of explicit consent

One of the most important privacy rules in the PSD2 Directive is that payment service providers may not have access to personal data without the consumer's explicit consent. This applies, for example, to account servicing payment service providers (such as banks) and payment initiation service providers.

The requirement of explicit consent requires, among other things, that a payment service provider requests consent from a consumer to gain access to his or her personal data, and this consent is obtained separately from other parts of the contract.

The way in which explicit consent is sought must be free, unambiguous, informed and specific. Consumers should also be able to withdraw their consent easily.

For example, someone should not be put under pressure to give consent. Furthermore, consent must be an active act; tacit consent or pre-ticked boxes are not permitted. A payment service provider must also properly inform a consumer as to which data is collected and for what purpose it is used.

To which payment service providers does this requirement apply?

The requirement of explicit consent for access to personal data applies to all types of payment services. The exception to this is if the service only consists of the provision of an account information service (but as soon as the account information service is combined with another payment service, the explicit consent requirement applies).

Payment service providers, like all other organisations, must also comply with the General Data Protection Regulation (GDPR). Important GDPR rules require, for instance, a payment service provider to have a legal basis to process personal data and must take measures to properly protect personal data.

Payment services

Payment service providers have access to consumers' payment details. These are often sensitive personal data. For example, data relating to the consumer's income and purchasing behaviour. Therefore, payment service providers must explicitly ask consumers for their consent. This is laid down in the second Payment Service Directive (PSD2).

Explicit consent

Explicit consent under PSD2 implies, among other things, that consumers must actively give the requested consent. This must be done separately from the other elements of a contract.

The consumer decides

Without explicit consent, the payment service provider cannot have access to the payment details of that consumer. The consumer therefore decides whether a payment service provider may have access to his or her accounts and payment behaviour.

About PSD2

PSD2 is a European Directive. Its aim is to promote innovative payment services and to protect the privacy of consumers.

In addition to the PSD2 Directive, payment service providers must also comply with the General Data Protection Regulation (GDPR).

General questions about PSD2

1. What is PSD2 about?

PSD2 stands for the second Payment Service Directive. It is a European directive for payment service providers. Among other things, this directive permits that not only banks but also other parties may have access to a payment account. These parties must have a license from De Nederlandsche Bank for this purpose.

Payment service providers may only gain access to personal data for the provision of a payment service if the consumer has given his explicit consent.

The same rules will apply everywhere in the EU. This will make it easier to offer and use these services. The rules in the directive have been transposed into Dutch law but this law is not currently in force yet.[1]

According to the bill, the Dutch data protection authority (**AP**) will supervise the rules of PSD2 that deal with privacy.

2. When does PSD2 enter into force?

The PSD2 directive has already entered into force but has yet to be transposed into Dutch legislation.

This is done by means of an implementation law. This law has now been adopted by the Lower House of Parliament and was subsequently submitted to the Senate.

The implementation act integrates the requirements of PSD2 into Dutch law and determines who supervises it.

The drafting of national PSD2 laws must take place in every EU country.

3. What is a payment service provider?

Payment service providers are companies that offer payment services or services that help to keep track of individual bank accounts.

Consumers, for example, can use such a company to make a payment via their mobile phone. Or to keep a personal financial accounting based on information from their bank account.

Sensitive personal data
PSD2 imposes requirements on payment service providers so that the service is secure. The protection of consumer privacy is an important element because payment details are sensitive financial personal data.

Explicit consent
Therefore, PSD2 requires that payment service providers can only access personal data with the consumer's explicit consent and then only to the extent that this data is necessary for the provision of the payment service.

Of course, consumers can only give this explicit consent for their own personal data.

Everywhere in the EU
If payment service providers comply with the PSD2 rules, they may offer their services anywhere in the EU. In this way, consumers can also use providers from other EU countries.

4. Why is there a directive specifically for payment service providers?

The special rules for payment service providers in PSD2 are made because payment data often contains sensitive information about a person's private life.

[1] Note from Bird & Bird LLP: please note that this is not entirely accurate. Formally the Directive has not yet been transposed into Dutch law as it is still pending approval by the Senate.

New payment services

More and more parties want to offer new types of payment services. This may include payment apps that give consumers an overview of their payment accounts with different banks or a convenient service that arranges payments itself.

PSD2 gives payment service providers the opportunity to develop new payment services. At the same time, the directive contains extra rules to protect the privacy of consumers.

Privacy legislation

Payment service providers, like all other organisations, must comply with the General Data Protection Regulation (GDPR).

5. What are the rules on supervision?

Four supervisors are involved in the supervision of payment transactions. In addition to the Dutch Data Protection Authority (AP), the DNB, ACM and AFM have a role to play.

The AP supervises the protection of people's privacy. In doing so, the AP looks at the requirements in the General Data Protection Regulation (GDPR) and the requirements included in PSD2.

DNB will be given the task of granting licenses to payment service providers. DNB's supervisory task is aimed at ensuring a stable financial system. Consultation and cooperation takes place with the AP in the interests of both the public and the business community.

The ACM looks at the competition between providers in the payments market and the bank's provision of access to account information.

The AFM plays an important role when a payment service provider also offers financial products or services (for example, providing credit to consumers). For this purpose, a license must be obtained from the AFM.

It goes without saying that the supervisory authorities work closely together. This is important both for the citizen (after all, it concerns their privacy protection) and for companies (who must of course have legal certainty).

6. What is the role of the AP with regard to the supervision of payment service providers?

The Dutch Data Protection Authority (AP) is the supervisory body for privacy legislation in the Netherlands. This privacy legislation is primarily governed by the General Data Protection Regulation (GDPR).

The AP also supervises the extra rules that apply to payment service providers. These are laid down in the second Payment Service Directive (PSD2).

AP advice on PSD2

In addition to being a supervisor, the AP is also tasked to advice on legislation. The AP has advised on PSD2 twice:

- In August 2017, the AP advised on the bill implementing PSD2. The two most important points were to clarify the relationship between GDPR and PSD2 and to clarify which supervisor must supervise the privacy requirements under PSD2. This was necessary so that people, companies and banks and supervisors know where they stand[2].
- In January 2018, the AP advised on the PSD2 implementation decree. The advice was to transfer the entire supervision of the protection of personal data in payment services to a single supervisor - the AP[3].

It is clear that the AP works closely with the regulators DNB, ACM and AFM to protect the privacy of payment transactions.

7. Do the same requirements apply throughout Europe for explicit consent?

Yes. Throughout the European Union the same requirements apply with respect to explicit consent.

The AP is a member of the European Data Protection Board (EDPB). All European privacy regulators are members of this European partnership.

EDPB's position on the protection of personal data by payment service providers is published in a letter on the EDPB website[4].

Questions of payment service providers about explicit consent under PSD2

1. In what situation does a payment service provider need to ask for explicit consent?

PSD2 has 3 types of consent:

- Explicit consent to the payment service provider's access to personal data;
- Explicit consent to the payment order or transaction;
- Explicit consent to access to the payment account for account information service providers.

With the latter two types of consent, the payment service provider asks whether another party may access that account, as the consumer has the payment account at the bank.

Please note: you may only request explicit consent to access personal data that are necessary for offering your payment service.

[2] Note from Bird & Bird LLP: the document is available here https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/advies_psd2.pdf (Dutch version only)
[3] Note from Bird & Bird LLP: an informal, English courtesy translation is provided by Bird & Bird LLP, and available here: https://www.twobirds.com/~/media/pdfs/dutch-dpa-letter-to-dutch-minstry-of-finance.pdf?la=en
[4] Note from Bird & Bird LLP: the letter is available here: https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf

2. To which payment service providers does the requirement of explicit consent apply?

The requirement to obtain explicit consent for access to personal data applies to all types of payment services. This is laid down in the PSD2 Directive. There is an exception for services that consist solely of offering an account information service.

Exception for account information services

The requirement to obtain explicit consent for access to personal data does not apply if the service consists solely of offering an account information service, such as a personal financial accounting service.

In such a case, however, the consumer must explicitly consent to the service. This is done via an authorisation[5] that is valid for a maximum of 90 days.

The account information service may not process personal data for purposes other than the provision of the account information service. The account information service must comply with all the rules of the General Data Protection Regulation (GDPR).

Please note that as soon as the account information service is combined with another payment service, for example a payment initiation service, the requirement of explicit consent for access to personal data applies.

3. What are the requirements of explicit consent?

The requirement of explicit consent means that you must ask a consumer for consent to process his or her personal data in an explicit way, i.e. separately from other parts of the contract.

In addition, the manner in which you request consent must meet the following requirements.

Free

As a payment service provider, you may not put pressure on anyone to give permission. A consumer must be able to refuse permission and must not suffer any disadvantage as a result.

Unequivocal

Granting permission must be a clear active act. For example, a (digital) written or oral statement. In any case, it must be absolutely clear that permission has been granted.

You may not assume tacit consent. The use of pre-ticked boxes is therefore not permitted.

Informed

You need to inform consumers about:

- The identity of the organisation that determines the purpose and means of the processing of personal data. This will be your organisation if it is the party responsible for processing.
- The purpose of each processing for which you request permission.
- What personal data you collect and use.
- The right of data subjects to withdraw their consent.
- You must provide this information in an accessible form and you must use clear language. So that someone understands the information and can make a well-informed decision.

[5] Note from Bird & Bird LLP: "authorisation" should probably read as "authentication".

Specific
Consent must always apply for a specific processing and a specific purpose.

Please note: as a payment service provider you can only request permission to access and process personal data that are necessary for offering your payment service.

Retractable
A consumer has the right to withdraw his consent. This must be as easy for the consumer as it was to give permission. For example, via a pop-up. You must inform a consumer about this before he or she gives permission.

Note: the consequence of revoking a previously given consent is that the consumer can no longer use your payment service as he or she might have been used to. You may, of course, inform the consumer of this in advance.

Accountability
You must be able to demonstrate that you have requested and received valid permission when the Data Protection Authority requests it. This is part of your accountability under the GDPR.

4. How must a payment service provider ask for explicit consent?

The requirement of explicit consent means that you ask a consumer for consent to process his or her personal data in an explicit way, i.e. separately from other parts of the contract. This can be done in various ways.

Tacit consent or requests to agree to the general terms and conditions of your payment service are not sufficient.

Separately from the other parts
In any case, you must ensure that the consumer, separately from the other parts of the contract, explicitly agrees to the access to his or her personal data.

In a digital environment, this can be done, for example, in the form of a separate window (such as a pop-up or a checkbox to be ticked in a dialogue). The consumer can then indicate in this box that he gives permission for access to his or her personal data.

No contract without permission
Did you not receive explicit permission? Then this will result in you not being able to perform the contract with the consumer. Of course, you may point this out to the consumer when asking for permission.

Other questions of payment service providers about PSD2

1. When can I process personal data?

As a payment service provider, you always need a basis from the General Data Protection Regulation (GDPR) in order to be allowed to process personal data. In addition, you must first have

obtained explicit permission from the consumer to gain access to his personal data with another payment service provider.

Explicit consent

As a payment service provider, you may not have access to a consumer's personal data without their explicit consent. This is laid down in PSD2.

Explicit means that you must clearly and explicitly ask a consumer for permission. The consumer must actively give the requested consent.

Please note: the requirement of explicit consent does not apply if you only offer an account information service and usually also not for contracts that have already been concluded.

The GDPR principles

The requirement of explicit consent from PSD2 applies in addition to the rules from GDPR. GDPR states that organisations must base the processing on one of the six GDPR principles for processing personal data. For you as a payment service provider, this will often be on the basis that the processing is necessary for the execution of the agreement.

Please note: one of the principles for processing personal data is 'consent of the person concerned'. This is not the same as the explicit consent as referred to in PSD2.

2. With which privacy provisions do I need to comply?

Some of the most important rules of GDPR are:

- You must have a basis for processing personal data.
- You may be required to appoint a Data Protection Officer (DPO).
- You may be required to perform a data protection impact assessment (DPIA).
- You must work in accordance with the principles of privacy by design and default.
- You must take measures to protect personal data properly.
- You may need to draw up a register of processing activities.
- You are obliged to inform consumers properly.
- Your systems, procedures and internal organisation must be geared to the privacy rights of consumers.

3. Does a payment service provider need to ask permission for current contracts?

No, in many cases this is not necessary. The explicit consent is about the payment service provider gaining access to personal data from another payment service provider. For example, a bank.

Within an existing contract, access to personal data at or by another party is usually not necessary.

In this context, an existing contract is understood to mean a contract that was concluded prior to the date on which Dutch legislation on the requirement of explicit consent will apply.

Does the existing contract require access to personal data of another party? Then you must still ask for the consumer's explicit consent.

Questions of consumers of payment service providers

1. How does a payment service provider obtain my personal data?

Payment service providers may only gain access to your personal data necessary to provide the payment services with your explicit consent.

In addition, payment service providers may not provide your personal data to other organisations without your consent.

2. Is a payment service provider able to look into my personal data if someone else gives consent?

Are you the beneficiary of a payment (is there someone else transferring money to you)? If so, the payment service provider can see personal details that are necessary to perform the payment service. For example, your name and bank account number.

No other data can be accessed without your explicit permission.
Giving permission in the case of commercial use
You can also only consent to the commercial use of your personal data by a payment service provider. For example, to analyse your purchasing behaviour.

Another person cannot give your personal data to a third party for commercial use without your permission.

3. How can I withdraw my consent?

You should be able to revoke your consent as easily as you have given it.

Your payment service provider must have clearly informed you that you can revoke your consent and also how you can do this. The payment service provider must have given you this information before concluding the agreement.

Please note: the consequence of revoking a previously given consent is that you may no longer be able to use the payment service as you were used to.

4. Can a payment service provider retain my personal data after withdrawing consent?

Yes, but only if necessary. The law states that personal data may not be stored longer than necessary.

Before concluding the agreement, your payment service provider must have informed you of how long it will store your personal data. Is this period over? In that case, the payment service provider must delete your personal data.

5. What are my options when my payment details are used without my permission?

Do you suspect that a payment service provider processes your personal data in a way that is contrary to the rules? Then first contact the payment service provider.

If you cannot find a solution together, then you can file a privacy complaint with the Data Protection Authority (AP). We handle every complaint. The way in which we do this differs depending on the type of complaint. You will always receive a response from the AP to your complaint.