



Note: Please read this document carefully and keep it in a safe place for future reference.

Notice of Variation for Retail Banking

This notice covers the following services rendered by HSBC France, Athens branch (the Bank) in accordance with Law 4537/2018 which transposes PSD2 EU 2016/2366 on payment services (PSD2)

- payment services including the transactional payment accounts and other relevant banking services
- the way you access your payment accounts and services online.

Our Bank's framework contract for payment services and our Bank's General Terms and Conditions for Individuals as well as the HSBC Internet Banking Service & HSBC Bank Mobile Banking App License terms and conditions have been amended to reflect changes that relate to the introduction of PSD2 in Greece.

You will be able to download the applicable new General Terms and Conditions (which includes) the framework contract for payment services, the Internet & Mobile Banking terms and conditions (the New Terms) and the Notice of Variation for Individuals from the Bank's public website at following link at (www.hsbc.gr/terms) or pick up a copy in our branches.

PSD2 replaces the first Payment Services Directive and aims to support innovation and competition in the payments' sector and increase the security of payment transactions. PSD2 sets out a common legal framework for us and our customers when making and receiving payments both within and outside the Union (EU) and/or the European Economic Area (EEA).

In Greece PSD2 is implemented through the Law 4537/2018 (the PSD2 Law).

Scope of application of the PSD2 Law

The first Payment Services Directive largely applies to payments in euro or another member state currency and relates to payment services where the payment service providers of both the payer and payee, or the one and only payment service provider of both the payer and the payee are/is located in the EU.

The PSD2 Law extends the scope of the regime so that the PSD2 Law will apply for:

- (a) Payment transactions carried out in the currency of an EU/EEA Member State, where the payment service provider of both the payer and the payee, or the one and only payment service provider for the payment transaction at issue are/is located within an EU and/or EEA Member State.
- (b) Payment transactions carried out in any currency, where the payment service providers of both the payer and the payee, or the one and only payment service provider for the payment transaction at issue are/is located within the EEA. The following articles of the PSD2 Law will not apply in this context: articles 45§1(b),

52(2)(e), 56(a) (relating to obligation of payment service providers for granting of information as to the maximum execution deadline for the rendering of payment services or the execution of an individual payment transaction) and articles 81 to 85 of the PSD2 Law (relating to the obligations of payment service providers as to the amounts transferred and/or the amounts received, the treatment of cases whereby the payee does not keep a payment account with the payment service provider or whereby cash is placed on a payment account).

- (c) Payment transactions carried out in any currency, where only the one of payment service providers of either the payer or the payee is located within the EEA. The following articles of the PSD2 Law will not apply in this context: articles 45§1(b), 52(2)(e), 52(5)(z) and 56(a) (relating to obligation of payment service providers for granting of information as to the maximum execution deadline for the rendering of payment services or the execution of individual payment transactions), article 62 §§ 2 and 4 (relating to applicable charges in the sense of the application of SHARE principle to payment transactions made within EU/EEA Member States and the non-entitlement of the payee to imposition of any charges on the use of any payment instrument), articles 76 and 77 (relating to the conditions for refund of amounts for payment transactions initiated by or other a payee and the submission of relevant refund requests), article 81 (relating to obligations of payment service providers as to the amounts transferred or the amounts received), article 83§1 (relating to the applicable deadline for crediting the payee's payment account), articles 88 and 91 (relating to the Bank's liability for non-execution, improper or late execution of payment transactions and recourse rights between payment service providers and correspondents).

In cases (b) and (c) above, the PSD2 Law will only apply to those parts of the payment transaction which are carried out within the EU and/or the EEA Member States.

Strong Customer Authentication Procedure, Security Measures for Confidentiality and Integrity of Personalized Security Credentials and Common and Secure Open Communication Standards.

In certain categories of payment transactions, including where the Customer:

- (a) accesses its payment account online;
- (b) initiates an electronic payment transaction; and
- (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses

we will implement a Strong Customer Authentication procedure in order to enhance security of payment transactions. The Strong Customer Authentication procedure is an authentication procedure that is based on the use of at least two separate elements out of the following categories: (a) an element that only the Customer knows (e.g. a password or a PIN code); (b) an element that only the Customer possesses (e.g. a card, a mobile phone or a token device); and (c) an element that is inherent to the Customer (e.g. a fingerprint or iris scan).

The aforementioned elements of Customer authentication/identification are independent, in the sense that the breach of one of the elements does not compromise

the reliability of the other elements and they are especially designed to ensure confidentiality and authentication of your data.

We may, upon circumstances, acknowledge some exemptions from the application of said strong customer authentication subject to specified and limited conditions based on the level of risk, the amount and the recurrence of the payment transactions and the payment channels used for its transaction. You will be notified of the specific elements constituting the strong customer authentication procedure, as well the scope of transactions which may be exempted from such requirement in due course.

We intend to implement appropriate security measures for the protection of the confidentiality and integrity of your personalized security credentials, including authentication codes, during all phases of the authentication as well as standards of common and secure open communication with both payment service users and payment initiation providers, account information providers and payment service providers issuing card-based payment instrument.

Such procedure and/or measures will be finalized in due course and will be duly notified to the Customer and will relate to the above channels of payment services when the respective terms will be accordingly amended.

Third Party Providers (TPPs)

We will provide access to certain information of your payment account to payment initiation service providers ("**PISPs**") or account information service providers ("**AISP**") (together referred to as Third Party Providers - "**TPPs**") lawfully performing payment initiation services and account information services in Greece or in an EU/EEA Member State and explicitly authorized by you to gain access to certain information of your payment account for the purpose of rendering payment initiation services and/or account information services (as the case may be). Such possibility only applies as to payment accounts that are accessible online and is subject to the presumed fulfilment of the requirements provided therefor under the PSD2 Law.

We may deny a TPP access to an account where there are objectively justified and duly evidenced reasons relating to unauthorised use or fraudulent activities by that TPP. Before doing so, we will inform you that we intend to deny access and will give reasons for doing so, unless it is not reasonably practicable to do so, in which case we will inform you immediately afterwards. In either case, we will inform you in the manner in which we consider most appropriate in the circumstances and will not be obliged to inform you, where doing so would compromise our reasonable security measures or otherwise be unlawful.

Confirmation on the availability of funds for execution of card-based payment transactions

Upon request of a payment service provider issuing card-based payment instruments where you have initiated a card-based payment transaction for a certain amount in your capacity as payer, we shall immediately confirm towards the payment service provider issuing card-based payment instrument explicitly authorized thereto by you on whether an amount necessary for the execution of the card-based payment transaction is available on your payment account, provided that the payment account of the Customer as payer is accessible online at the time of the

request and relevant requirements under the PSD2 Law are fulfilled. The confirmation on availability of funds to be given by us in such context shall consist only in a simple 'yes' or 'no' answer and not in a statement of the account balance, and it shall not allow us to block funds on your payment account. Said obligation of us shall not apply to payment transactions, the initiation of which is conducted by the payment service user through a card in which electronic money is stored.

Payer's liability for unauthorized payment transactions

In case of unauthorized payment transactions, you in your capacity as a payer shall be liable up to a maximum of € 50, for losses arising from the use of a lost or stolen or misappropriated payment instrument. Such liability will not apply in cases where (a) the loss, theft or misappropriation of the payment instrument was not detectable to by the payer prior to the conduct of the payment transaction, except where the payer has acted fraudulently or (b) the loss was caused by acts or omissions of the Bank's/our employee, an agent or a branch or of an entity to which the Bank/we had/have outsourced its/our activities.

Furthermore, the payer is liable for all losses related to unauthorized payment transactions, provided that these losses are due to fraud or failure to comply with one or more of his obligations with regard to the payment instruments and the personalized security information deliberately or as a result of gross negligence, in which case the above amount specified in this term shall not apply.

The payer will not bear the financial consequences deriving from use of lost or stolen or misappropriated payment instrument as of the moment the Bank is notified thereof by the payer, unless the latter acted fraudulently.

Liability in case of payment initiation services for non-execution, defective or late execution of payment transactions

Where a payment order is initiated by the payer through a PISP, the Bank shall, subject to the certain cases (i.e. where the payer did not report to the payment service provider without delay, in good time and appropriately that he had become aware of an unauthorized or erroneously executed payment transaction, where the exclusive unique identifier provided by the payment service user was erroneous and in the case of absence of liability due to unusual and unforeseeable circumstances which are beyond the control of the party invoking them) refund the amount of the non-executed or defective payment transaction to the payer and, where appropriate, it shall restore the debited payment account to the state in which it would have been had the defective/erroneous payment transaction not taken place.

Where the PISP is liable for the non-executed, defective or late execution of a payment transaction, it shall compensate immediately the Bank, upon the latter's request, for all losses sustained by the latter or any money amounts paid by the latter in the context of said refund to the payer.

Payment transactions where the transaction amount is not known in advance

In case of a payment transaction initiated by or through the payee where the exact amount is not known at the moment you provide your consent for the execution of the payment transaction, you acknowledge that we may block funds on your payment account only if you provide us with your consent for the exact amount of funds to be blocked. We will then release the blocked amount without undue delay after receipt of information relating to the exact amount of the payment transaction.

The value date of incoming payments

With regard to incoming payment transactions, we will ensure that the amount of the payment transaction is made available once credited to your account, the value date being no later than the working day following its receipt, provided that:

- (a) there is no currency conversion; or
- (b) there is one currency conversion between the euro and a EU/EEA Member State currency, or between two EU/EEA Member State currencies.

This obligation shall also apply in case where we act as payment service provider also for the payer of the payment transaction.

The SHARE principle

With regard to charges on payment transactions, we apply a “SHARE” principle with regard to payment services granted within a Member State of the EU and/or the EEA, where both the payer’s and the payee’s payment service providers are, or the one and only payment service provider with respect to the payment transaction is, located within a Member State of the EU and/or the EEA. This means that you pay the charges we impose and the payer or payee respectively will pay the charges imposed by its payment service provider, without this meaning that the two charges must be equal.

Alternative Dispute Resolution (ADR) procedure, complaints handling procedure and information on consumer rights

We have established a specific complaints’ resolution procedures as to any complaints which may arise in the context of rendering payment services, which will enable a time-efficient addressing thereof. Notwithstanding this, you remain always entitled to submit a complaint to General Secretariat of Commerce and Consumer Protection as well as to have recourse to the competent Alternative Dispute Resolution (ADR) bodies, including the Independent Authority Consumers’ Ombudsman and the Banking and Investment Services Ombudsman. We will also keep you informed on your rights as consumer within the parameters of the PSD2 Law.

Questions and concerns

If you have any questions about the provision of any payment services covered by the PSD2 Law, you should direct your question to your client services relationship manager.

How we use your personal information

Our systems rely on having the customer information to duly prevent, detect and address cases of fraudulent and unauthorized transactions, safeguard the safety and genuity of payment instructions and secure against financial crime. This includes, where applicable, collecting up-to-date information of you and other persons relating to you.

You acknowledge as payment service user that our performance of payment services on your behalf entails the processing, to the extent applicable, of your data and/or persons related to you, and, by signing and/or accepting the Bank's General Terms and Conditions (including the framework for payment services), you grant your explicit consent to us for collection and processing, to the extent applicable, of your data and/or data relating to persons related to you and to the payment order and payment transaction itself, for rendering of such services and the discharge of any legal obligations arising from the applicable laws. You also explicitly acknowledge that the processing, to the extent applicable, of your data and/or the data of persons related to you and to the payment order and payment transaction itself, also encompasses cases of providing access to certain information of your account to TPPs and payment service providers issuing card-based payment instruments explicitly authorized by you for gaining access in the context of rendering payment initiation services and account information services or verification of the availability of sufficient funds on your payment account for the execution of initiated card-based payment transactions.

You acknowledge that our performance of payment services on your behalf entails the processing, to the extent applicable, of your data and/or persons related to you, and, by signing and/or accepting the General Terms and Conditions for Individuals (including the framework contract for payment services), you grant your explicit consent to us for collection and processing, to the extent applicable, of your data and/or data relating to persons related to you and the payment order and transaction itself, for rendering of such services and the discharge of any legal obligations arising from the applicable laws. You also explicitly acknowledge that the processing, to the extent applicable, of your data, also encompasses cases of providing access to certain information of your account to TPPs and payment service providers issuing card-based payment instruments explicitly authorized by you for gaining access in the context of rendering payment initiation services and account information services or verification of the availability of sufficient funds on your payment account for the execution of initiated card-based payment transactions.

You can find further information from our Privacy Notice at the Bank's public website and branches.

In all cases you may submit any objections to the New Terms until 27.08.2018, in writing at any of our branches, otherwise your non-opposition until that date is equivalent to your acceptance of the New Terms.