Information accompanying transfers of funds

2013/0024(COD) - 11/03/2014 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 627 votes to 33 with 18 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds.

Parliament's position adopted at first reading under the ordinary legislative procedure amended the Commission proposal as follows:

Flows of illicit money, a major problem for the Union: Parliament stressed that flows of illicit money damage the structure, stability and reputation of the financial sector and threaten the internal market as well as international development, and directly or indirectly undermine the confidence of citizens in the rule of law. The funding of terrorism and organised crime remains a significant problem, which should be addressed at Union level.

Scope: Members state that the regulation shall not apply to transfers of funds carried out using a credit, debit or prepaid card or voucher, or a mobile telephone, e-money, or any other digital or information technology (IT) device where the card or device is used to pay goods and services to a company within professional trade or business. However, it shall apply when the means of payment is used in order to effect a person-to-person transfer of funds.

Information accompanying transfers of funds: before transferring the funds, the payment service provider of the payer shall apply customer due diligence measures and shall verify the accuracy and completeness of the information.

In the case of transfers of funds not made from an account, the payment service provider of the payer is required to verify at least the name of the payer for transfers of funds of up to EUR 1 000. It shall verify the complete information relating to the payer and the payee where the transaction is carried out in several operations that appear to be linked or where they exceed EUR 1 000.

Transfers within the Union: where the payment service provider(s) of both the payer and the payee are established in the Union, only the full name and the account number of the payer and the payee or the unique transaction identifier shall be required to be provided at the time of the transfer of funds.

In the case of an identified higher risk the payment service provider of the payee require the complete information relating to the payer and to the payee.

Missing information on the payer and the payee: from a practical perspective, Members consider that some kind of verification is going to be required, in order to avoid frauds and assure that the person who receives the funds is in fact the payee designated by the payer.

Where the payment service provider of the payer is established in a third country that presents an increased level of risk, enhanced customer due diligence shall be applied.

In any event, the payment service provider of the payer and the payment service provider of the payee shall comply with any applicable law or administrative provisions relating to money laundering and terrorist financing.

The **intermediary payment service provider** should have effective procedures in place in order to detect not only whether information is missing but also **incomplete**, in particular if numerous payment services are involved to improve the traceability of transfers of funds.

Obligation of cooperation: payment service providers and intermediary payment service providers shall **respond fully and without delay**, to enquiries exclusively from the authorities responsible for combating money laundering or terrorist financing of that Member State concerning the information required under the Regulation. Specific safeguards shall be put in place in order to ensure that such exchanges of information comply with data protection requirements. No other external authorities or parties shall have access to the data stored by the payment service providers.

Because a great proportion of illicit financial flows ends up in **tax havens**, Parliament states that the Union should increase its pressure on those countries to cooperate in order to combat such illicit financial flows and improve transparency.

It is also proposed that payment service providers established in the Union shall apply this regulation with regard to their **subsidiaries and branches** operating in jurisdictions outside the Union that are not deemed equivalent.

Data protection: Members stressed that:

- payment service providers shall carry out their tasks for the purposes of this Regulation in accordance with national law transposing Directive 95/46/EC. Data retained shall in no case be used for commercial purposes;

- **the transfer of personal data to a third country**, or to an international organisation, which does not ensure an adequate level of protection may take place only after prior authorisation by the supervisory authority;

- information on the payer and the payee shall **not be kept any longer than strictly necessary** . Records of information shall be kept for a maximum period of five years and upon expiry of this period, personal data must be deleted.

Data protection authorities shall have powers, including the indirect access powers, to **investigate, either ex officio or based on a complaint,** any claims as regards problems with personal data processing.

In any case, access to the information collected shall be reserved only to designated persons or limited to persons strictly necessary for the completion of the undertaken risk.

Sanctions and monitoring: the Commission is called on to **submit a report to the European Parliament** , by 1 January 2017, on the implementation of the regulation, in particular, the application of Chapter IV, with regard to sanctions and monitoring.

EBA may issue guidelines on the processes for implementing the Regulation, taking into account the best practices of Member States.

Members also suggested that the Commission strengthen cooperation with national authorities outside the Union responsible for investigation and sanctioning breaches such as repeated non-inclusion of required information on the payer and payee by a payment service provider