

Position Paper

of the German Insurance Association

ID number 6437280268-55

**on Article 5(2) and (3) of the revised EU Directive on
Payment Services (PSD2) (professional indemnity insurance
for payment initiation and account information services)**

**Gesamtverband der Deutschen
Versicherungswirtschaft e. V.**

German Insurance Association

Wilhelmstraße 43 / 43 G, 10117 Berlin
P.O. Box 08 02 64, 10002 Berlin

51, rue Montoyer
B - 1000 Brussels
Phone: +32 2 28247-30
Fax: +32 2 28247-39

Contact:

Dr. Mareike Lohmann
Business Administration and
Information Technology
Phone: +49 30 2020-5451
E-mail: m.lohmann@gdv.de

Sabine Pareras
Liability, Credit, Marine and Aviation
Insurance, Statistics
Phone: +49 30 2020-5314
E-mail: s.pareras@gdv.de

www.gdv.de



I. Introduction

As a major user of payment services for the purpose of executing premium and loss payments, the German insurance industry has a strong interest in clear, reliable and sustainable rules for payments. Accordingly, we have closely monitored the agreement on the revised Directive on Payment Services (PSD2).

From the point of view of liability insurers, Article 5(2) and (3) of PSD2 are of particular interest. According to Article 5(2) and (3), Member States shall require undertakings that apply for authorisation as a payment initiation service provider (PISP) and undertakings that apply for registration as an account information service provider (AISP) to submit evidence that they “hold a professional indemnity insurance [...] or some other comparable guarantee [...]”. These alternative requirements had not been brought into the legislative procedure until the negotiations in the Council started, which has resulted in the fact that the German insurance industry did not have the opportunity to comment on the introduction of the new indemnity insurance.

We would like to point out that the required insurance cover might be difficult to realise. It might be possible that insurance capacity will be restricted. Accordingly PISPs and AISPs might face difficulties to obtain insurance cover or they might obtain insurance cover only at high risk premiums.

The higher the requirements applying to the insurance, the more difficult the coverage by means of indemnity insurance will probably be. This should be taken into account when outlining the requirements that shall apply to the indemnity insurance.

II. On the considerations of liability insurers in detail

1. Potential increase in risks in relation to payment transactions

Depending on the requirements for common and secure open standards of communication, the security of authentication, which is a major issue of online payments, might be weakened considerably as the result of involving third-party service providers. The Federal Financial Supervisory Authority (BaFin) has also addressed this issue¹. Similar statements were made by the German Banking Industry Committee, amongst others, in the context of its press release on the trilogue agreement published in May.

¹http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1406_zahlungsdiensterichtlinie_II_en.html

The risk of hacker attacks (man-in-the-middle attacks, social engineering and phishing attacks) would consequently rise. Insurers, however, have strong reservations about the coverage of damages caused by the hacking of the technical systems in the context of cyber risk insurance for financial services, or even believe that this risk is to be excluded from insurance cover.

2. Insurance coverage does not compensate for a lack of risk preparedness

Insurance coverage is no substitute for inadequate or even missing technical provisions. The focus should be on providing security rather than on providing insurance. The actual technical outline of the account interface to the account servicing payment service providers is essential in this context.

At present, it is for the European Banking Authority (EBA) to define the requirements for common and secure open standards of communication, in particular with regard to the authentication of and the secure communication between the relevant actors. When outlining the regulatory technical standards (RTS) to be established, the highest security standards have to apply to the authentication procedure as well as to the technical design of the interface. The insurance industry calls for uniform requirements in this context, which allows for coherent, interoperable communication between third-party service providers and banks in Europe. The requirements shall not be so general as to allow for the development of different standards on the market. Otherwise, risk assessment by the insurance undertakings would be made even more difficult. The issue of whether the authentication information issued by the account servicing payment service provider will be disclosed to the third-party service provider will also be crucial for the risk assessment.

In addition, relevant obligations need to be specified, for instance, it must be stipulated that the customer only enters authentication information on a website agreed upon by the undertaking that issues the authentication information and the customer in advance.

3. Substantial liability risks to be covered

According to Article 5(2) of PSD2, the scope of cover of the professional indemnity insurance or of the comparable guarantee respectively to be provided for PISPs shall apply to the liabilities as specified in Articles 73, 89, 90 and 92. In the case of AISPs (cf. Article 5(3)), the liability of the service provider resulting from non-authorised or fraudulent access to or

non-authorized or fraudulent use of payment account information shall be covered. The standards of liability stipulated with regard to PISPs, in particular, provide for a very strict no-fault liability regime.

The liability risks to be covered are consequently considered to be substantial. For instance, the possibility of an unauthorized access to sensitive data of thousands of payment service users due to a lack of adequate security measures cannot be ruled out. A huge number of unauthorized payment transactions could be executed as a result. Such large loss scenarios make the calculation of risks extremely difficult and would pose enormous challenges for insurers.

Moreover, it may be doubted whether a significant number of PISPs and AISPs will actually take out professional indemnity insurance pursuant to PSD2 in the future. In principle, however, a specific number of risks would be a necessary condition for ensuring a sufficient spreading of risks in the portfolio of the insurer.

4. Necessary framework conditions for professional indemnity insurance in accordance with Article 5(2) and (3) of PSD2

Insurers must be able to stipulate adequate provisions in the insurance contract. This has to be taken into account when outlining the requirements applying to the insurance cover. The following aspects of the scope of cover, in particular, are to be considered:

- The requirements applying to the sum insured must not be excessive.
- It is absolutely essential that an annual aggregate limit with regard to the sum insured can be established in the insurance contract.
- It must be possible to agree on a time limitation of the insurance cover. It might be possible that insurance can be provided only on a claims made basis.
- Policyholders and insurers must be allowed to agree on an adequate deductible and the application of risk-relevant exclusions. E.g. intentional neglect of duty by the insured and fraudulent acts which are committed by the insured have to be excluded from PII coverage.

III. Executive Summary:

The definition of the requirements for common and secure open standards of communication (see 2 above) and to the insurance cover (see 4 above) is of particular importance to the insurability of the risks. It is currently not possible to predict whether sufficient insurance capacity will be available for PISPs and AISPs in the future. Therefore, there is an urgent need to promote the possibility of covering risks by means of some other comparable guarantee. The provision of guarantees or the assumption of liability by financially strong undertakings might be applied for this purpose.

Berlin/Brussels, 28 January 2016