Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR

-

Public consultations

Dear Madam / Dear Sir,

First of all a heartfelt thank you from the financial sector for shedding some light into the interplay of the Second Payment Services Directive (Hereinafter ,,PSD2'') and the GDPR. As you are aware, financial institutions (and especially banks) have been subject to a tremendous amount of regulation over the past decade whether in the form of Mifid II, GDPR, PSD2 or governance related matters published by the European Banking Authority (Hereinafter ,,EBA''). Publishing guidelines like these truly helps in identifying the nuances that arise for financial institutions to tackle.

Alas, our question concerns the processing of biometric data for the purposes of carrying out strong customer authentication (Hereinafter ,,SCA''). Having in mind that explicit consent under the PSD2 does not correspond to explicit consent under the GPDR and that payment service providers have a legal obligation to carry out SCA consisting of three elements. If a payment service provider as the data controller has a legal obligation to carry out the assessment of an individual's characteristics (as per the Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 – inherence shall be interpreted as the biometric characteristics of an individual), then in our point of view explicit consent for the purposes of processing biometric data for SCA, cannot be held as an adequate legal basis for such processing. Since all three elements of SCA (possession, inherence and knowledge) are equally important (SCA requiring 2/3 regardless of which), conditioning the use of inherence by explicit consent under the GDPR simply puts it on unequal grounds compared to the other two elements.

With EBA's unwillingness to commit to a statement on the issue of biometrics under the PSD2 in order to convey a technologically neutral standpoint, payment service providers are left in the dark due to the limitations of explicit consent under the GDPR. This has resulted in many financial institutions relying on on-device biometrics of Apple or other smartphone manufacturers to fulfil the aspect of SCA inherence. While such interpretation of the law may be user friendly in essence, it is questionable whether payment service providers may solely rely on fulfilling this requirement in potential legal proceedings where the identity of the person carrying out the transaction is disputed as multiple fingerprints and faces may be registered per device. (The device only answers with the information whether the person carrying out the transaction at that moment in time is the person whose biometric data is stored in the device's secure enclave – with multiple fingerprints stored the person is not directly identifiable.)

If financial institutions have a legal obligation to carry out SCA where the element of inherence is conditioned by explicit consent under the GDPR and where payment service providers have adopted a restrictive meaning of inherence, is such consent truly freely given?

Guidance on this issue would be very welcome.

Kindest regards,

Tibor Gogh

Všeobecná úverová banka, a.s.
Mlynské nivy 1, 829 90 Bratislava 25,
Obchodný register: Okresný súd Bratislava I
Oddiel: Sa, vložka číslo: 341/B, IČO: 31320155
VÚB je členom skupiny INTESA SANPAOLO