WIRTSCHAFTSKAMMER ÖSTERREICH

Abteilung für Finanz- und Steuerpolitik
Wiedner Hauptstr. 63 | Postfach A-1045
Wien
T +43 (0) 5 90 900-DW | F + 43 (0) 5 90 900-113739
E Erich.Kuehnelt@wko.at
W http://wko.at

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
	FSP/Mag. Erich Kühnelt	3739	16.09.2020

Konsultation der Leitlinien zum Verhältnis DSGVO und PSD2

Zur Konsultation des Europäischen Datenschutzausschusses (EDSA) zu Leitlinien zum Verhältnis der DSGVO zur PSD2 nehmen wir wie folgt Stellung:

keine separate Datenschutzfolgeabschätzung
Die angeführte Datenschutzfolgenabschätzung würde einen erheblichen administrativen Mehraufwand bedeuten. Das Erfordernis einer separaten Datenschutzfolgenabschätzung sollte gestrichen werden, weil bei den in den Leitlinien skizzierten Zahlungsvorgängen nicht mehr passiert als bei unserem "normalen" Zahlungsverkehr, nur, dass letzterer durch jemand anderen angestoßen wird. **Daher sehen wir keinen Grund diese separate Datenschutzfolgeabschätzung durchführen zu müssen (die bei ungünstigster Auslegung für jeden Zahlungsdienstleister extra vorgenommen werden müsste), weil der Zahlungsverkehr per se ohnehin schon bewertet werden muss.**
Zu Punkt 5.1 Z 52, letzter Satz wird festgehalten, dass kein Erfordernis nach einer DPIA besteht, da das Mapping bereits mit Inkrafttreten der DSGVO erfolgt ist. Der Satz “most probably, a Data Protection Impact Assessment (DPIA) will be required in accordance with article 35 GDPR, which will help in this mapping exercise” sollte gestrichen werden.

Zustimmung des PSU an TPP / Privacy Dashboard / Hindernis

Die Leitlinien empfehlen in Punkt 77, dass ein ASPSP (kontoführende Bank) dem PSU (Zahlungsdienstenutzer) bestimmte selbst vorzunehmende Datenschutzeinstellungen ermöglicht; die Datenschutzeinstellungen sollten eine Übersicht der TPP, denen der PSU seine ausdrückliche Zustimmung erteilt hat, enthalten. Im Sinne der Leitlinien sollte der ASPSP dem PSU die Möglichkeit bieten, seine Zustimmung an den/die TPP zu widerrufen, was die Verweigerung des Zugriffs durch den jeweiligen TPP zur Folge hätte. Die Leitlinien merken in diesem Zusammenhang an, dass solche Datenschutzeinstellungen, die dem PSU die Möglichkeit bieten, seine ausdrückliche Zustimmung an TPP zu erteilen oder diese zu widerrufen, keine Hindernisse für die TPP darstellen dürfen.

Bekanntlich darf der ASPSP das Vorliegen einer ausdrücklichen Zustimmung durch den PSU an einen konkreten TPP nicht überprüfen, weil dies nach der Rechtsansicht der EBA und der

Europäischen Kommission ein Hindernis darstellt. Allfällige Datenschutzeinstellungen, durch welche der ASPSP dem PSU ermöglicht, eine Zustimmung an einen TPP zu erteilen, kommen aus zahlungsverkehrsrechtlicher Sicht daher nicht in Frage.

Allerdings kann der PSU sowohl nach der Rechtsansicht der EBA als auch des EDPB vom ASPSP verlangen, dass der ASPSP einem oder mehreren bestimmten TPP den Zugriff verweigert. Der PSU kann dem TPP seine Zustimmung aber jederzeit neuerlich erteilen und die Überprüfung der Zustimmung durch den ASPSP stellt idR ein Hindernis dar. **Es stellt sich daher die Frage, ob der ASPSP aus datenschutzrechtlicher Sicht nach dem Widerruf der Zustimmung durch den PSU in den Datenschutzeinstellungen des ASPSP – bevor der ASPSP dem TPP neuerlich Zugang gewährt – von dem jeweiligen TPP den Nachweis einer neuerlichen ausdrücklichen Zustimmung durch den PSU verlangen kann/muss, ohne dass dies ein Hindernis darstellen würde**.

Zugriff auf Daten, die für das Erbringen des TPP-Zahlungsdienstes nicht notwendig sind
Im Sinne des Grundsatzes der Datenminimierung sollte der Zugriff des TPP auf jene Daten beschränkt werden, die für das Erbringen der jeweiligen Zahlungsdienste (entweder AIS oder PIS) notwendig sind (Punkt 61).

In der Praxis verlangen die TPP den Zugang zu allen Daten, zu welchen auch der PSU Zugang hat. In diesem Zusammenhang verlangen beispielsweise die PISPs den Zugriff auf bereits gezeichnete (aber noch nicht ausgeführte) Transaktionen mit dem Argument, dass sie wissen müssen, ob ausreichende Deckung für die von ihnen auszulösende Zahlung vorhanden ist, obwohl den PISPs (Zahlungsauslösedienstleister) sowohl der Kontostand als auch der Disposaldo angezeigt wird.

Der PISP sollte auf die Transaktionsdaten keinen Zugriff haben, weil diese für seinen Zahlungsauslösedienst nicht notwendig sind (er sieht den Disposaldo). **Es ist daher eine Klärung durch EDPB erforderlich, ob der ASPSP aus datenschutzrechtlicher Sicht den Zugriff des TPP auf solche Daten, die für die Erbringung seines Zahlungsdienstes objektiv nicht erforderlich sind, verweigern kann/muss, ohne die Bestimmungen der PSD2 zu verletzen.** Wer beurteilt allerdings die objektive Notwendigkeit der Daten für die Vertragserfüllung durch den TPP

Zu beachten ist in diesem Zusammenhang ferner, dass es sich hier um eine besondere Frage der Ausgestaltung und des Designs der, den TPP zur Verfügung zu stellenden Schnittstelle handelt. Da sich aus den Erfahrungen der Praxis heraus die meisten Änderungen bei dieser Schnittstelle als besonders zeit- und kostenaufwändig darstellen, ist es ein wesentliches Anliegen, über den Inhalt und den Umfang der über diese Schnittstelle den TPP zur Verfügung gestellten Daten Rechtssicherheit zu haben, um damit unnötige Kosten in Programmierungen zu ersparen.

Zugriff auf Daten, die keine Zahlungskonten betreffen
Die Leitlinien stellen auch klar (Punkt 64), dass TPP keinen Zugriff auf Daten haben dürfen, die nicht Zahlungskonten betreffen; die PSD2 sei nämlich keine rechtliche Grundlage dafür, um den TPP Zugang zu Spar- oder Kreditkonten zu gewähren.

Die TPP verlangen in der Praxis jedoch auch den Zugang zu Konten, die keine Zahlungskonten sind; hierzu nutzen die TPP die Methode des Screen Scraping. **Da die PSD2 keine Rechtsgrundlage für den Zugang zu diesen Daten darstellt, ist eine Klärung erforderlich, ob der ASPSP den Zugang zu nicht Zahlungskonten betreffenden Daten durch Screen Scraping aus datenschutzrechtlicher Sicht unterbinden muss bzw. unter welchen Voraussetzungen ein solcher Zugang den TPPs gewährt werden darf.**

Müsste etwa der PSU aus datenschutzrechtlicher Sicht eine ausdrückliche Zustimmung an den ASPSP erteilen (iSd Art 6 Abs 1 lit a DSGVO), um einem konkreten TPP (AISP) den Zugang zu den Kredit- oder Sparkonten des PSU gewähren zu dürfen? Darf/muss der ASPSP dem TPP den Zugang zu solchen Daten ohne den Nachweis einer ausdrücklichen Zustimmung des PSU verweigern, ohne dass dies ein Hindernis darstellt?

Zu erwähnen ist, dass es technisch gar nicht möglich ist, einem TPP, der sich via Screen Scraping über die Kundenschnittstelle Zugriff in das Internetbanking eines Kunden verschaffen will, dauerhaft daran zu hindern, da aus der Perspektive des ASPSP derartige Zugriffe wie Zugriffe des Kunden selbst sind. Aus diesem Grund muss natürlich jegliche Strafsanktion gegenüber ASPSP für den Fall, dass einem TPP der Zugriff via Screen Scraping nicht unterbunden wird, vorweg entschieden abgelehnt werden."

Einwilligung gemäß Art 94 (2) PSD 2
Von besonderer Bedeutung ist der die Einwilligung gem. Art 94 (2) PSD2 betreffende Abschnitt (Punkt 3, Z 28 bis 43). Die Aussage, dass die Einwilligung gem. PSD2 sich von jener nach DSGVO unterscheidet sowie die diesbezüglichen Ausführungen der europäischen Datenschutzbehörde, werden begrüßt. In Z 36 der Guidelines ist festgehalten, dass „explicit consent" iSd Art 94 (2) PSD2 als vertragliche Einwilligung zu verstehen ist. Weiters wird in Z 38 der Guidelines festgehalten, dass Art 94 (2) nicht Rechtsgrund für die Verarbeitung von persönlichen Daten ist. Zudem ist die PSD2 in Kohärenz mit der DSGVO zu verstehen.
Die Guidelines versuchen deutlich zu machen, dass Zahlungsverkehrsdaten nicht aufgrund einer ausdrücklichen Einwilligung gem. Art 94 (2) PSD2, sondern aufgrund der DSGVO (Grund ist Vertragserfüllung) verarbeitet werden. Die ausdrückliche Einwilligung des Kunden gem Art 94/2 PSD2 sieht die Datenschutzbehörde in Zusammenwirkung mit der DSGVO somit lediglich dafür als erforderlich an, dass der Zahlungsdienstnutzer bei Vertragsunterzeichnung separat ausgewiesen darüber informiert werden muss, welche seiner persönlichen Daten wofür verarbeitet werden und er darin ausdrücklich einwilligen muss. Um Missverständnisse bei den Adressaten der Guidelines zu vermeiden, wird angeregt, die Guidelines dahingehend zu ergänzen, dass der Rechtsgrund der Verarbeitung von Zahlungsdaten die Vertragserfüllung gem. DSGVO darstellt.

Um zu vermeiden, dass tatsächlich zu jedem Zahlungsauftrag eine gesonderte Einwilligungserklärung des Auftraggebers zur mit dem Zahlungsauftrag verbundenen Datenverarbeitung eingeholt werden muss, wäre es idZ wichtig, dass der EDPB in den Leitlinien klarstellt, dass die explizite Zustimmung im Sinne des Art 94 (2) PSD2 dann nicht erforderlich ist, wenn die Datenverarbeitung nur Daten betrifft, die der Kunde zur Durchführung der von ihm beauftragten Zahlungsaufträge bekanntgegeben hat oder die dem Zahlungsdienstleister schon bekannt sind und die er im Zuge der Auftragsbearbeitung weitergeben muss.

Punkt 4a (silent party data) betreffend wird vorgeschlagen, deutlich auszuführen, dass technische Pflichten der Drittdienstleister nicht den Banken überbunden werden dürfen. Es ist die Aufgabe der Drittdienstleister, den Schutz der Daten technisch sicherzustellen und nicht die Aufgabe "aller beteiligten Parteien".

Zu Punkt 5a (special categories of data) wird angeregt, zu verdeutlichen, dass sich die Datenkategorie nicht zB aus dem Verwendungszweck eines Zahlungsvorgangs oder der Identität eines an einem Zahlungsvorgang Beteiligten ergeben kann. Ein derartiger Filter ist technisch nicht möglich. Die besondere Datenkategorie muss sich weiterhin aus dem Zweck der jeweiligen Datenverwendung ergeben.

Die Ausführungen zur Verarbeitung sensibler Datenkategorien in den Leitlinien können dahin verstanden werden, dass Zahlungsaufträge, die sensible Daten beinhalten, nur aufgrund gesonderter ausdrücklicher Einwilligungserklärung bearbeitet werden dürften. Die diesbezügliche Analyse der eingehenden Zahlungsaufträge und die Einholung der Einwilligungen wären mit erheblichen administrativen Aufwänden verbunden. Es wäre daher auch hier notwendig, dass der EDPB in den Leitlinien klarstellt, dass die beschriebenen Anforderungen nicht gelten, wenn die Datenverarbeitung nur Daten betrifft, die der Kunde zur Durchführung der von ihm beauftragten Zahlungsaufträge bekanntgegeben hat oder die dem Zahlungsdienstleister schon bekannt sind und die er im Zuge der Auftragsbearbeitung weitergeben muss.

Punkt 6a (usage of digital filters) wird vorgeschlagen, zu präzisieren, dass die Einrichtung der digitalen Filter eine Verpflichtung der Drittdienstleister darstellt und es nicht sachgerecht wäre, diese Pflicht bei den Kreditinstituten zu sehen.

further remarks

No. 3 Please clarify whether the Guideline applies to all payment services pursuant to Annex 1 PSD2, or solely to the newly created payment services pursuant to Annex 1 numbers 7, 8 PSD2.

No. 12 For the sake of legal certainty, please provide examples under what circumstances a payment service provider could be regarded as a data processor. We believe that a financial service provider can never be regarded as data processor, if and as long as it provides services under a license issued by a financial markets authority and renders these services within the statutory framework of a financial regulatory law. It is not up to the data subject to determine the purposes and means of this processing.

No. 15 It is not clear what is meant by the second sentence. Please amend.

No. 23 The data protection board wrongly assumes in section 23 of the guidelines that third-party providers are subject to the Anti Money Laundering Directive. We would like to point out that this Directive does not apply to third-party providers. Third-party providers do not carry out any due diligence measures with regard to the anti money laundering directive.

No. 28-43 We are aware that Art 94 (2) PSD2 expressly states the requirement of an "*explicit consent*". Still, we want to take the opportunity to point out the irrationality of this clause and its incongruity within the context of Union law:

- The provision of payment services is a regulated financial service.
- Payment service providers (PSP) need to obtain a license issued by the relevant national competent authority and are subject to their monitoring.
- The legal relation between PSPs and payment service users (PSU) is mainly regulated by PSD2. The technical components for the provision of payment services is regulated, among others, by the SEPA-regulation (260/2012/EU), the SEPA-Credit Transfer Rulebook (issued by the European Payments Council) and the Regulation on the Transfers of Funds (2015/847/EU).
- This tight regulatory corset does not leave room for any deviations by single PSPs – on the contrary: the "inflexible", schematic and heavily standardized payment infrastructure is the

reason why it is possible to transfer money within one day (or within seconds in the scope of SEPA INST) throughout the whole European Union.

- If a PSU wants to make use of fast and reliable payment services, he/she has to get into a contractual relationship with a licensed PSP.
- The amount of personal data which gets processed for the provision of payment services is also regulated and standardized (see for example https://www.stuzza.at/en/payment-transactions/payment-transfer-formats.html).
- All this is regulated by law, industry standards and framework contracts. It is counterintuitive why the PSU has to provide an additional "consent", **to something that is not even up to his/her discretion**. If the PSU does not "consent" to the processing of his/her data, he/she simply cannot make use of the payment services. There is no legal or factual way to render payment services (i.e. open an account, transfer money, etc) without the processing of personal data. A "forced" consent would also have **detrimental effects for the general public's understanding of GDPR**, because one of the main concepts of a consent ("freely given") would suddenly be scrapped when it comes to payment services.
- In addition, the access to a payment account is an enforceable right within the EU (Art 15, 16 Directive 2014/92/EU). Making the access to an account or the rendering of basic payment services conditional to a consent, runs counter to Directive 2014/92/EU.
- In the light of all this, it is our strong believe that it is sufficient to provide the PSU with the *information* that and which of his/her data is processed when making use of payment services. It should be clarified by the EDPB that **the PSU does not have to "consent" to the processing, if the processing of personal data is necessary for rendering payment services**.

No 50-57 We are aware of the high standards the GDPR sets for the processing of sensitive data. However, please consider the practical consequences of this specific part of the guideline:

- Data qualifying as "sensitive" in the sense of Art 9 GDPR can only occur while processing payment services if the PSU actively chooses to do so: (1) Either by his or her choice of words in the free-text-fields provided in the payment reference etc or (2) by means of the quality of the beneficiary of the payment (i.e. the recipient).
- However, (2) is not as clear as it seems at the first instance: If, for example, a PSU were to transfer money to a "Cancer Treatment Center", this alone does by no means reveal any sensitive data. Maybe he/she is in perfect health and participated at a workshop or an awareness program hosted by the Center; maybe he/she donated the money. Another example: If a PSU were to transfer money to a Political Party, it may be the exact opposite of his/her revealing his/her political beliefs: Maybe he/she lost a defamation battle in court *against* the Polititcal Party (i.e. they represent *not* his/her beliefs) and now has to pay damages.
- Regarding (1) – free text fields – there remains ambiguity as well.
    - If a German speaking PSU enters "Krebs" in the free text field of the payment reference, does he/she refer to the disease ("cancer"), the zodiac sign ("Cancer"), the family name ("Krebs") or the animal ("Crab"/crustacean)?
    - If the PSU is versed in a foreign language that is *not* spoken in the PSP's country of residence – either because he/she is an expat, a refugee, etc – and composes the payment reference in this language - how is the PSP supposed to even realize that a free-text field contains sensitive data?
    - If a PSU makes a transfer to a Hospital with the reference "Cancer Treatment Bill no. 12345", maybe he/she pays the bill for his/her daughter, his/her spouse or a friend.
- Therefore, the approaches suggested in the Guideline (asking for explicit consent or implementing technical measures) do not seem practicable.
- We believe that the processing of sensitive data for the sole purpose of rendering payment services **is of substantial public interest (Art 9(2)(g) GDPR)**:

  - The need for a smooth operation of payment systems is enshrined in the Treaty on the Functioning of the European Union itself (Art 127).
  - The integrated internal market for safe electronic payments is crucial in order to support the growth of the Union economy and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit fully from the internal market (Recital 5 PSD2).
  - Payment services are essential for the functioning of vital economic and social activities. (Recital 7 PSD2).
  - An integrated market for electronic payments in euro, with no distinction between national and cross-border payments is necessary for the proper functioning of the internal market (Recital 1 SEPA-Regulation).
  - SEPA is regarded as essential for the Europe 2020 strategy which aims at a smarter economy in which prosperity results from innovation and from the more efficient use of available resources (Recital 2 SEPA-Regulation)
  - Banking (i.e. ASPSP) is considered a critical infrastructure by Directive (EU) 2016/1148.
  - The smooth functioning of the internal market and the development of a modern, socially inclusive economy increasingly depends on the universal provision of payment services (Recital 3 Directive 2014/92/EU).
  - The access to a payment account is an enforceable right within the EU (Art 15, 16 Directive 2014/92/EU).
  - Without PSPs and the infrastructure provided by them, the Europe's economy would crash within the blink of an eye.
- This shows that the provision of payment services and the associated processing of data are of a **substantial public interest**. It is appropriate to the aim pursued (only such sensitive data are processed that the PSU him-/herself chooses to disclose), PSD2 respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (see esp Art 66, 67 PSD2).
- Hence, the **processing of sensitive data in the course of rendering payment services** as defined in Annex 2 of the PSD2 **does not require the PSU's explicit consent nor is there a need to "filter" sensitive data**.
- Obtaining the PSU's consent would also run counter to the PSP's obligation to a maximum 1-day execution time pursuant to Art 78 PSD2, or the even shorter execution time of less than 60 seconds when the payment order is executed within the SCT Inst scheme. As to the transaction volume, the share of SCT Inst scheme in the total volume of SCT was 5.92% in Q1 2020 (compared to 1.02% in the Q1 2019).

No 63,64 Please note that ASPSPs are obliged to not alter or modify the data that AISPs/PISPs are accessing. Digital filters and similar measures would be in breach of Art 32(3) Commission Delegated Regulation (EU) 2018/389. See also the European Banking's Authority opinion on said Regulation (EBA-Op-2018-04, page 4 and number 18).

Freundliche Grüße

Mag. Erich Kühnelt