[redacted]

[redacted]

Gesendet von meinem BlackBerry 10-Smartphone.
Von: Rebekka Weiß
Gesendet: Mittwoch, 3. Juli 2019 18:01
An: Ziegner, Jan (VII A 5)
Betreff: Bitkom Anmerkungen zur GwG-Novelle

Sehr geehrter Herr Ziegner,

wir kennen uns leider noch nicht persönlich, gern wollte ich aber noch einmal mit Ihnen hinsichtlich der GWG Novelle in Kontakt treten. Wir konnten leider durch verschiedene Faktoren bedingt nicht im Rahmen der Konsultationsfrist die geplanten Änderungen des GwG kommentieren. Jedoch sind in unserer Mitgliedschaft einige Bereiche sehr direkt betroffen; neben den Kreditinstituten auch die Identifizierungsdienstleister sowie die DLT- und IaaS-Anbieter. Ich wollte daher die Gelegenheit nutzen mit Ihnen zumindest noch in dieser Phase unsere Bitkom-internen Überlegungen teilen.

Insgesamt ist uns wichtig herauszustellen, dass wir die zeitige Umsetzung ins nationale Recht natürlich begrüßen, wir aber Bedenken haben ob der aktuelle Textvorschlag nicht ein Innovationshemmnis für die in Deutschland regulierten Institute werden könnte. Ich habe hier einige offene Diskussionspunkte zusammengefasst und würde mich freuen, wenn wir uns dazu noch einmal austauschen könnten. Gerne auch telefonisch.

1. Offener Diskussionspunkt

Hinsichtlich der Pflichtangaben für Ausweisdokumente haben wir in unserer Mitgliedschaft diskutiert, ob die „ausstellende Behörde“ tatsächlich eine Pflichtangabe sein muss oder ob dies nicht optional gestaltet werden könnte. In der EU werden zunehmend auch ID-Karten ausgegeben, die die „ausstellende Behörde“ gar nicht mehr als Pflichtangabe führen.

2. § 11a GwG-Neu

Aus wettbewerblichen Gesichtspunkten haben wir weiterhin den § 11a GwG-Neu analysiert. Uns erscheint problematisch, dass er einer Nutzung der bei Banken vorhandenen Identifizierungsdaten der Kunden z.B. zur Registrierung bei einem Vertrauensdiensteanbieter zwecks Erstellung eines qualifizierten Zertifikates entgegensteht. Dies stellt nach unserer Ansicht jedoch – solange das VideoIdent-Verfahren umstritten und auf Grundlage der Verfügung beschränkt bleibt und eID-Dienste noch nicht flächendeckend nutzbar sind – die derzeit einzige Möglichkeit dar, qualifizierte Signaturen massenfähig zu machen. Unter anderem sehen wir kritisch „(1) Verpflichtete nach § 2 verarbeiten personenbezogene Daten in Erfüllung ihrer Sorgfalts- und Meldepflichten auf Grundlage dieses Gesetzes ausschließlich für Zwecke der Verhinderung von Geldwäsche und Terrorismusfinanzierung. Eine Verarbeitung zu anderen Zwecken ist nicht zulässig.“ Damit werden sämtliche Folgegeschäftsmodelle faktisch unnutzbar gemacht. Die Bank/der Verpflichtet muss daher die

personenbezogenen Daten aus der Identifizierung außerdem zum Zweck der Führung der Geschäftsbeziehung mit dem Kunden speichern/verarbeiten dürfen.

Der sich im Umbruch befindlichen und zunehmend dynamischen digitalen Finanzmarktplatz Deutschland nicht in seinem Wachstum zu behindern. Gerade bei KYC-Prozessen im Rahmen des Kunden-Onboarding besteht noch erhebliches Verbesserungspotential. Viele Kunden brechen langwierige und mit Medienbrüchen verbundene Identifizierungsverfahren erfolglos und frustriert ab. Dies führt nicht zu einer verbesserten Geldwäscheprävention, sondern einzig zu vermindertem Wettbewerb im Finanzdienstleistungssektor. Neue Anbieter und innovative Zahlungs- und Identitätsdienstleister werden durch die sich aus unnötig mühsamen Kontoeröffnungsprozessen ergebenden Lock-In Effekte benachteiligt. Wir befürchten, dass die in Deutschland regulierten und niedergelassenen Zahlungsinstitute durch die vorgeschlagenen Änderungen des GwG einen erheblichen kompetitiven Nachteil gegenüber EU- und außereuropäischen Wettbewerbern erleiden. Dies gilt insbesondere für die in § 11 a Abs. 1 S. 2 GwG-E und § 17 Abs. 3 a GwG-E vorgeschlagenen Änderungen, die zum Teil erheblich über die Vorgaben der 4. EU-Geldwäscherichtline hinaus gehen.

Auch aus datenschutzrechtlichen Gesichtspunkten wirft der § 11 a GwG-Neu Fragen auf. Die Regelung ist insoweit problematisch, als sie nicht klarstellt, dass jedenfalls ein Teil dieser Daten eben gerade nicht nur wegen des GwG erhoben wird. Kreditinstitute sind zB auch nach der AO verpflichtet, Angaben zu ihren Vertragspartnern (zu steuerrechtlichen) Zwecken zu verarbeiten. Darüber hinaus ist es auch nach dem HGB verpflichtet, Vertragspartner zu kennen und jedenfalls diese Daten festzuhalten. Schließlich werden Kundendaten wie der Name und die Anschrift auch zur Erfüllung der vertraglichen Pflichten des Kreditinstituts gegenüber seinen Kunden benötigt, weshalb sie von den Kunden auch zu diesem Zweck zur Verfügung gestellt werden. Hier muss unbedingt klargestellt werden, dass - soweit die Daten auch aus anderen Zwecken erhoben werden und verarbeitet werden dürfen - die hier aufgenommene Einschränkung nicht gilt, sondern die allgemeinen Regeln des Datenschutzes, die durchaus in gewissem Rahmen eine Zweckänderung erlauben. Dies gilt insbesondere für § 11 a Absatz 1 Satz 2 RefE des GwG. Ohne eine solche Klarstellung ist künftig möglicherweise streitig, ob ein Verpflichteter die Adresse seines Vertragspartners z. B. für Anschreiben zu Werbezwecken nutzen darf (was nach derzeitiger datenschutzrechtlicher Grundlage unstreitig der Fall ist, solange der Kunde nach Wettbewerbsrecht nicht widersprochen hat).

§ 11 a Absatz 1 Satz 2 RefE-GwG könnte hinsichtlich des Wortlauts z.B. wie folgt angepasst werden: „...eine Verarbeitung zu anderen Zwecken ist ohne eine andere Rechtsgrundlage nicht zulässig“. Jedenfalls die Einwilligung des Kunden muss hier stets möglich sein. Der Betroffene hat das Recht, selbst zu entscheiden, ob er seine Daten anderswo hingegeben haben möchte. Insoweit könnten auch eigene Interessen der Vertragspartner bestehen. Die DS-GVO stellt die Autonomie und Hoheit des Bürgers über seine Daten in den Mittelpunkt. Das Verbot des § 11 a Abs. 1 S. 2 GwG-E würde bei wörtlicher Auslegung selbst solche Datenverarbeitungsvorgänge verbieten zu denen der Nutzer dem Verpflichteten eine wirksame separate Einwilligung erteilt hat. Dem Verpflichteten wäre es daher selbst dann untersagt, die in Erfüllung ihrer Sorgfaltspflichten erhobenen personenbezogenen Daten zu verarbeiten, wenn eine wirksame separate Einwilligung des Nutzers in die Datenverarbeitung vorliegt oder sich eine Rechtfertigung aus anderen von der DS-GVO anerkannten Zwecken ergibt, z.B. anderweitig berechtigtes oder vertragliches Interesse.

3. § 17 Absatz 1 GwG-Neu

Zu unter 2. Bereits angesprochenen Thematik möchten wir zudem noch ergänzen, dass selbst der nach § 17 Abs. 1 GwG vorgesehene Rückgriff eines anderen GwG-Verpflichteten auf einen „Dritten“ (z.B. ein GwG-Verpflichteter, der die erstmalige GwG-konforme Identifizierung eines Nutzers durchgeführt hat) bei strenger Auslegung des § 11 a Abs. 1 S. 2 GwG-E in Frage gestellt würde.

4. § 17 Absatz 3 a GwG-Neu

Hinsichtlich der Ausführung der Sorgfaltspflichten durch Dritte begrüßen wir die Möglichkeit zur Erfüllung eigener Sorgfaltspflichten auf Dritte zurückzugreifen. Insbesondere im Bereich der Identifikation des Kunden, z.B. bei Begründung einer Geschäftsbeziehung, kann die Vermeidung wiederholten Identifizierungsaufwandes zu einer erheblichen Wettbewerbsverbesserung durch einfachere Konteneröffnungen und damit -wechsel sowie zu erheblichen Kosteneinsparungen führen. Der „Lock-In-Effekt", der sich aus unnötig aufwändigen Kontoeröffnungsprozessen ergibt, kann erheblich reduziert werden.

Die klarstellenden Änderungen zum Territorialprinzip (S. 85 f. des Referentenentwurfs) sind grundsätzlich nachvollziehbar und entsprechen der Umsetzungssystematik der 4. GW-RL. Jedoch möchten wir die Sorge zum Ausdruck bringen, dass durch die neu eingefügten Beschränkungen zum Rückgriff auf „verpflichtete Dritte" gemäß § 17 Abs. 3 a GwG-E, innovative deutsche Zahlungs- und Identitäts-Dienstleister einen erheblichen kompetitiven Nachteil gegenüber EU- und außereuropäischen Wettbewerbern erleiden. Soweit ersichtlich bestehen in keinem anderen EU-Land derartig strikte Anforderungen beim Rückgriff auf andere Verpflichtete zu Erfüllung der eigenen Sorgfaltspflichten. Der vorgeschlagene § 17 Abs. 3 a GwG geht weit über die Regelung des Art. 25 der 4. GW-RL hinaus.

Der in § 17 Abs. 3a Nr. 2 GwG gewählte 24 Monatszeitraum wurde bereits während den Anhörungen zu den AuAs kontrovers diskutiert. Es ist weiterhin kein Maßstab oder eine durchgreifende Erklärung ersichtlich, warum im Rahmen einer „lebenden" Geschäftsbeziehung eines Instituts mit seinem Kunden 24 Monate als sicherer Zeitraum gelten sollen, 36, 48 oder 60 Monate jedoch nicht. Die durchgehenden Überwachungserfordernisse gegenüber seinen Kunden und den jeweiligen Zahlungsströmen, die ein reguliertes Institut zu erfüllen hat, ergeben über die Zeit ein sehr viel konkreteres Bild über die Identität eines Kunden als eine Erstidentifizierung. Eine Gesetzesnovelle hat andere Zwecke zu erfüllen als die Auslegungs- und Anwendungshinweise (AuAs) der BaFin. Während bei den AuAs eine konkrete Nennung von Details und Zeiträumen, wie z.B. dem Monatszeitraum aus § 17 Abs. 3 a Nr. 2 GwG-E hilfreich ist und den regulierten Instituten Leitplanken in der praktischen Anwendung des Gesetzes vorgibt, birgt eine derartig strikte Festlegung von Zeiträumen im Rahmen eines abstrakten Gesetzes das große Risiko, dass auf Veränderungen im Marktumfeld, z.B. durch technologische Innovationen und anderweitige Disruptionen nicht ausreichend schnell reagiert werden kann.

Die Gesetzesbegründung zu § 17 Abs. 3 a GwG-Neu umfasst das Verbot der „Kettenweitergabe" (S. 86 des Referentenentwurfs). Der Gesetzgeber übernimmt die Maßgabe der BaFin aus den AuAs, dass ein Rückgriff auf einen Dritten zu Erfüllung eigener Sorgfaltspflichten nur auf solche Dritte zulässig ist, die die Erstidentifizierung des Kunden durchgeführt haben. Begründet wird dies mit einer Vermeidung der „Fehlerpotenzierung" (S. 86 des Referentenentwurfs). Es ist unter Antigeldwäsche und Datenschutzgesichtspunkten richtig, nur Verpflichteten nach geldwäscherechtlichen Vorschriften die mehrfache Nutzung von Identifikationen zu gestatten. Das kontinuierliche Monitoring im Rahmen einer „lebenden" Geschäftsverbindung (S. 86 des Referentenentwurfs), inkl. der Überwachung und Aktualisierung des Identitätsdatensatzes durch regulierte Institute ist ein Kernaspekt funktionierender Geldwäschebekämpfung. Die regulierten Institute stellen eine der Säulen der Geldwäsche und Terrorismusbekämpfung dar. Zwar bedarf es im aktuellen Überwachungssystem durchaus auch der Überwachung durch eine Aufsichtsbehörde. Die verpflichteten Institute, mit ihren Anti- Geldwäschebeauftragten und geschulten Mitarbeitern sind jedoch ein wesentlicher Teil des Systems zur Verhinderung der Geldwäsche und Terrorismusfinanzierung. Umso unverständlicher ist daher die Maßgabe, dass „eine Übermittlung der Informationen immer nur durch den erstidentifizierenden Dritten erfolgen kann" und eine „Kettenweitergabe" von Informationen nicht gestattet wird. Das vermeintliche Risiko einer „Fehlerpotenzierung" wird nicht weiter belegt.

Die konkreten Auswirkungen auf den Crypto-Bereich und die Auswirkungen auf die Compliance-Anforderungen analysieren wir derzeit noch im Detail. Gern würde ich mich dazu noch einmal kurzfristig mit Ihnen austauschen.

Beste Grüße

Rebekka Weiß

Rebekka Weiß, LL.M.
Leiterin Vertrauen & Sicherheit

T +49 30 27576-161 | M +49 151 17439698 | Twitter: @Bitkom_Privacy

Mailsignatur <https://www.bitkom.org/>

cid:image002.jpg@01D0B566.16B72F60 <http://www.twitter.com/Bitkom>
Bitkom_Mailsignatur_Icon_Facebook <https://www.facebook.com/Bitkom/>
Bitkom_Mailsignatur_Icon_Instagram <https://www.instagram.com/bitkom_ev/>
Bitkom_Mailsignatur_Icon_XING <https://www.xing.com/company/bitkom>
Bitkom_Mailsignatur_Icon_LinkedIN <https://www.linkedin.com/company/bitkom-e-v-/>

Sie möchten verschlüsselte Mails an mich senden? Sie können dazu meinen S/MIME Public Key downloaden <https://www.bitkom.org/zertifikate/r.weiss.zip>

-

INVALID HTML