Europäischer Datenschutzausschuss
Rue Wiertz 60
B-1047 Brüssel

Absender	Mag. Christina Steininger
Telefon	+43 50811 2729
Fax	+43 50811 2709
E-Mail	christina.steininger@kapsch.net
Datum	24. November 2020 Daten6b3/CS

Feedback zu „Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data“ des Europäischen Datenschutzausschusses

Sehr geehrte Damen und Herren,

Die Kapsch TrafficCom AG erlaubt sich im Zusammenhang mit dem vorliegenden Entwurf des Europäischen Datenschutzausschusses wie folgt Stellung zu beziehen:

- **Einleitung:**

Die Auseinandersetzung auf EU-Ebene zu der seit Jahren bestehenden Problematik bzgl. der Datenübermittlung in ein Drittland und die daraus resultierende Handlungsempfehlung des Europäischen Datenschutzausschusses ist sehr zu begrüßen, allerdings führt dies nicht zu dem erhofften vollständig akkordierten Handlungsvorgehen und daher nicht zu dem langersehenten Einklang zwischen europäischen Datenschutzanforderungen und Praktikabilität im Alltag.

- **Zu den einzelnen Bestimmungen des Entwurfs**

Ad 2.3. Schritt 3:

Mit Einführung der Datenschutzgrundverordnung wurde das langjährige Ziel ein einheitliches europäisches Datenschutzgesetz zu schaffen um nationale Abweichungen möglichst zu unterbinden, erreicht. Durch die im 3. Schritt dieser Empfehlung beschriebenen case-by-case Beurteilungen, die für jede Datenübermittlung in ein Drittland vom Datenexporteuer selbst vorzunehmen sind, wird dieser Zugang der Vereinheitlichung wieder zunichte gemacht: Diese Entscheidungen müssen nun vom Datenexporteuer selbst getroffen werden. Jegliche individuelle Beurteilung führt zu unterschiedlichen Ergebnissen und birgt im unternehmerischen Kontext somit auch das Risiko von Wettbewerbsverzerrungen bzw.-nachteilen, da jene Unternehmen, die sich ernstlich mit diesen Handlungsschritten auseinander setzen und sich an Vorgaben und Empfehlungen halten, benachteiligt sind im Vergleich zu jenen, die Datenschutz nicht konform umsetzen und sich dadurch sowohl einen Wettbewerbs- als auch kommerziellen Vorteil verschaffen.
Zusätzlich zu dieser Wettbewerbsverzerrung ist die angedachte individuelle Beurteilung ein enormer Kostentreiber für jedes Unternehmen, da es die Pflicht des Datenexporteuers zu sein scheint, die

nationalen Vorschriften des im Drittland ansässigen Datenimporteur zu prüfen um sich als Datenexporteur zu vergewissern, ob nationale Vorschriften mit der Datenschutzgrundverordnung im Einklang sind und somit die Datenübermittlungen in ein Drittland durchgeführt werden können. Die eben beschriebenen Nachteile, die sich für ein redliches Unternehmen aus dieser case-by-case Entscheidung ergeben, können und dürfen nicht toleriert werden, vielmehr muss es auch weiterhin Ziel sein eine einheitliche europäische Vorgabe dahingehend zu entwickeln.

Ad 2.4. Schritt 4:

Zusätzliche Maßnahmen, seien sie technischer, organisatorischer oder vertraglicher Natur, können in der Theorie einen Datentransfer in ein Drittland durchaus legitimieren. Hält man sich allerdings vor Augen, dass der Abschluss erweiterter Standardvertragsklauseln als vertragliche Maßnahme nationales Recht, dem der Datenimporteur unterliegt, wohl nie aushebeln kann, zeigt diese Tatsache, dass eine Erweiterung der Standardvertragsklauseln dahingehend, dass z.b. der Datenimporteur den Betroffenen oder den Datenexporteur bei Zugriff auf die Daten des Betroffenen informieren muss, sollten Behörden zugreifen, in der Praxis nicht durchführbar ist, sofern nationales Recht (des Datenimporteurs) eine In-Kenntnissetzung untersagt.
Selbige Divergenz zwischen Theorie und Praxis ergibt sich beim Einsatz entsprechender technischer und organisatorischer Maßnahmen: Während eine Verschlüsselung in einer „Cloud“ und die damit einhergehende Unmöglichkeit eines Zugriffs durch Dritte in der Praxis noch machbar ist, ist das bei SaaS-Diensten schlicht unmöglich, denn diese Diensteanbieter können ohne Zugriff auf Echtdaten ihre vertraglichen Verpflichtungen in den meisten Fällen nicht erfüllen. Auch zeigt die praktische Erfahrung, dass die von Datenschutzbehörden oftmals geforderte Auswahl einer Alternative zu Anbietern in Drittstaaten nicht umsetzbar ist, da es für ein Vielzahl an standardisierten Produkten (Office-Lösungen, CRM, etc.) keine gleichwertige Lösung auf dem europäischen Markt gibt.

Ad Punkt 79 Bedingung 2:
Eine Bewertung der technischen Möglichkeiten öffentlicher Stellen, insbesondere von Geheimdiensten, um Verschlüsselungsmaßnahmen zu umgehen, ist dem Datenexporteur, aber auch dem Importeur nicht zuzumuten. Es handelt sich dabei in den allermeisten Fällen um streng geheime Informationen, jeder Versuch einer Bewertung wäre pure Spekulation.

Ad Punkt 79 Bedingung 4:
Viele kryptografische Algorithmen werden als OpenSource implementiert und verwendet. Die Sicherheit beruht in der Offenheit und Einsehbarkeit der Implementierung, eine formale Verifikation findet in der Regeln nicht statt. Falls der Einsatz von OpenSource Implementierungen von kryptografischen Algorithmen erwünscht ist, sollte auf diese wenig formale Art der Verifikation eingegangen und diese explizit erlaubt werden.

Ad Punkt 84 Bedingung 2:
Siehe Kommentar zu Punkt 79 Bedingung 2.

Ad Punkt 84 Bedingung 4:
Diese Anforderung schränkt die zu verwendenden Kryptografie-Algorithmen nicht begründbar auf asymmetrische Algorithmen ein und schließt ein Vertrauen auf die Authentizität eines Schlüssels durch andere Verfahren (z.B. persönliche Übergabe) aus. Diese Anforderung sollte daher allgemeiner formuliert

werden, sodass das Ziel, nur authentische Schlüssel zu verwenden, auch auf anderen Wegen erreicht werden kann.

Ad Punkt 84 Bedingung 9:
Sieh Kommentar zu Punkt 79 Bedingung 4.

Ad Punkt 84 Bedingung 10:
Diese Anforderung ist in der Realität leider nicht erfüllbar und zwar von niemandem. Der Fall des Schweizer Unternehmens Crypto AG zeigt, dass Geheimdienste es zum Teil sogar schaffen Backdoors in hochsichere, zertifizierte Verschlüsselungslösungen einbauen zu lassen.

- **Abschließende Anmerkung**

Mit diesen aktuellen Empfehlungen läuft man Gefahr, dass viele europäische Unternehmen Datenschutz in Zukunft ignorieren (müssen), da die datenschutzkonforme Umsetzung eines Datentransfers in ein Drittland schlicht nicht möglich ist. Die gegenwärtigen Probleme und Herausforderungen aufgrund des Datentransfers in ein Drittland lassen sich auch durch die Empfehlung gewisser Maßnahmen nicht negieren - ganz im Gegenteil - sie werden aufgrund der nicht vorhandenen Alternativen auf dem Europäischen Markt auch weiterhin bestehen.

Zu überdenken ist in diesem Empfehlungsdokument auch, dass ein risikobasierter Ansatz völlig außer Acht gelassen wird, obwohl er in der Datenschutzgrundverordnung durchaus Niederschlag gefunden hat. Viel realitätsnaher wäre die Ermöglichung der Durchführung einer Risikobewertung mit der Abwägung wie hoch die Wahrscheinlichkeit ist, dass personenbezogene Daten, die von Europa in ein Drittland transferiert werden, von ausländischen Überwachungsbehörden tatsächlich gefordert werden. Erst wenn dieses Risiko tatsächlich besteht und als hoch eingestuft wird, sollten strikte technische Maßnahmen wie zb. eine strenge Verschlüsselung ergriffen werden müssen. De facto macht der Hinweis in den Empfehlungen, dass vertragliche und organisatorische Maßnahmen wohl nicht ausreichend sein werden und technische Maßnahmen immer ergriffen werden müssen, jeden Transfer in ein Drittland unrechtmäßig was nicht Ziel dieses Empfehlungsschreibens sein kann.

Abschließend ist noch anzumerken, dass man durch dieses starre, nicht flexible Empfehlungsdokument die Gefahr in Kauf nimmt, dass die in den letzten Jahren geschaffene Awareness bzgl. Datenschutz wieder schwinden wird, da es für Datenexporteure schlicht nicht möglich sein wird Datenschutzkonformität bei Datenübermittlungen in ein Drittland herzustellen.

Mit freundlichen Grüßen
Kapsch TrafficCom AG

Mag. Günter Wildmann
Chief Privacy Officer
Kapsch Group

Mag. Christina Steininger
Legal Counsel