Dr. Sergey Lagodinsky
MITGLIED DES EUROPÄISCHEN PARLAMENTS
Erster stellvertretender Vorsitzender im Rechtsausschuss

Rechtliche und politische Aspekte mobiler Applikationen bei der Bekämpfung der COVID19-Pandemie (Stand 24.04.2020)

Zusammenfassung: Aus europarechtlicher Perspektive ist die Anwendung der Bluetooth-Technologie für die Kontakt-Verfolgung im Rahmen der COVID-Krise nur dann zu unterstützen, wenn effektive Freiwilligkeit, strikte Zweckbindung, zeitliche Befristung sowie Dezentralisierung der Datenspeicherung gewährleistet sind. Darüber hinaus muss eine ganzheitliche Betrachtung der Auswirkungen der App-Funktion für die Betroffenen Bürger*innen beachtet werden. Rechtliche, soziale und psychologische Auswirkungen der Kontaktbenachrichtigung müssen vor der Einführung geklärt werden.

Die Gegenwärtige Diskussion um die Anwendung der Applikation im Rahmen der COVID-Bekämpfung wirft rechtliche und politische Fragen auf. Im Folgenden wird dazu aus europäischer Perspektive Stellung genommen. Nach der Schilderung rechtlicher Abwägungen (I) und Zusammenfassung verschiedener Applikations-Optionen (II), wird eine rechtliche und politische Bewertung (III) vorgenommen.

I. Grundsätzliche rechtliche Abwägungen

a. Rechtsgrundlagen für die Beurteilung:

Die rechtliche Beurteilung richtet sich nach der Datenschutzgrundverordnung (DSGVO) sowie der ePrivacy-Richtlinie (im Folgenden „Richtlinie")[1]. Letztere gilt als lex specialis zur DSGVO[2] für Umgang mit Daten auf elektronischen Geräten und Portalen, während die DSGVO für Rechte und Pflichten davor und danach gelten kann. Abgesehen vom unterschiedlichen Geltungsbereich hat die Unterscheidung auch Relevanz in Bezug auf die Rechtsdurchsetzung, da die Zuständigkeit für die Durchsetzung der DSGVO-Bestimmungen bei den unabhängigen Datenschutzbehörden[3] im jeweiligen Land liegt und Sanktionen festgelegt sind. Bei der Durchsetzung der ePrivacy-Richtlinie kann hingegen jeder Staat die Umsetzungsmodalitäten und Zuständigkeit selbst ausgestalten. Darüber hinaus gelten Art. 7, 8 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta" genannt), Art. 8 Abs. 1 der Europäischen Menschenrechtskonvention, 16 Abs. 1 des

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02002L0058-20091219&qid=1587367962627&from=EN

[2] Opinion of the Board 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

[3] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_de

Büro Dr. Sergey Lagodinsky MdEP Rue Wiertz 60 ASP 8H255 B - 1047 Brüssel
Tel.: +32 228 459 12 E-Mail: sergey.lagodinsky@europarl.europa.eu

Vertrags über die Arbeitsweise der Europäischen Union, die über entsprechende Öffnungsklauseln oder Verweise in den Erwägungsgründen der DSGVO bzw. Richtlinie direkt einbezogen sind, aber auch darüber hinaus gelten.

b. Rechtliche Maßstäbe für die Bewertung

Ausgehend von den erwähnten Rechtsgrundlagen gelten folgende Bewertungsmaßstäbe:

1. Für den Umgang mit „mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten" gilt Artikel 5 der **ePrivacy-Richtlinie**. Hiernach ist für jede Verwendung der Daten, einschließlich der Verkehrsdaten durch andere als dem/der Nutzer*in selbst, eine ausdrückliche Einwilligung des Betroffenen erforderlich (Abs. 1). Diese Einwilligung ist nur nach Erhalt ausführlicher Informationen über den verantwortlichen Verarbeiter sowie die Zwecke der Verarbeitung zulässig (Abs. 2). Für die „Speicherung von Informationen oder (den) Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind" sieht Abs. 3 strenge Voraussetzungen, insbesondere eine Einwilligung der Betroffenen vor.

2. Gemäß Art. 6 sind die erhobenen Verkehrsdaten zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden. Beide Vorschriften stehen jedoch unter dem Vorbehalt des Art. 15, der für besondere Fälle der öffentlichen Sicherheit Ausnahmen zu den oben genannten Grundsätzen zulässt, dazu zählen auch die Fälle von Art. 13 der Richtlinie 95/46/EG, die mittlerweile durch DSGVO abgelöst ist. Die Gründe für solche Ausnahmesituationen sind eng auszulegen. In Frage kämen im Falle der Pandemie allenfalls folgende Gründe aus Art. 13 der Datenschutzrichtlinie: (f) Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt bestimmte Zwecke verbunden sind; sowie (g) Rechte und Freiheiten anderer Personen.

3. Sogar dann, wenn eine Ausnahmesituation nach Art. 15 ePrivacy-Richtlinie angenommen wird, gelten gemäß EuGH **strenge Anforderungen an die Ausnahmemaßnahmen**, da diese auch in einer Krisensituation im Lichte der europäischen Bürger- und Menschenrechte ausgelegt und überprüft werden müssen[4]. Hierbei sind vor allem das Recht auf Privatheit sowie der Schutz personenbezogener Daten zu berücksichtigen (Art. 7, 8 der Charta), deren Einschränkbarkeit sich wiederum nach Art. 52 Abs. 1 der Charta richtet. Das bedeutet, dass Einschränkungen der Datenschutzrechte auch in Ausnahmesituationen nur auf Grund eines Gesetzes und lediglich zu Zwecken des Gemeinwohls oder zum Schutz der Rechte Dritter erlaubt sind, darüber hinaus aber notwendig und verhältnismäßig sein müssen und nicht das Wesen der Freiheitsrechte tangieren dürfen.

   Der EuGH leitet daraus den **Grundsatz der Datenminimierung** ab, wonach die Erhebung zeitlich begrenzt und auf „das absolut Notwendige" beschränkt wird[5]. Mit Blick etwa auf eine Vorratsspeicherung von Daten müsste eine Begrenzung etwa ein „geographisches Kriterium gewährleisten, wenn die zuständigen nationalen Behörden aufgrund objektiver Anhaltspunkte annehmen, dass in einem oder mehreren geografischen Gebieten ein erhöhtes Risiko besteht", dass bestimmte Taten vorbereitet oder begangen werden[6].

[4] EuGH EuZW 2017, 153, Rz. 91
[5] EuGH aaO Rz 109
[6] EuGH aaO Rz. 111

Büro Dr. Sergey Lagodinsky MdEP Rue Wiertz 60 ASP 8H255 B - 1047 Brüssel

Tel.: +32 228 459 12 E-Mail: sergey.lagodinsky@europarl.europa.eu

4. Ähnliche Kriterien bestimmt die DSGVO. Die Verordnung ist einerseits strenger, wenn es um den Umgang mit Gesundheitsdaten geht (deren Verarbeitung ist prinzipiell verboten – Art. 9 Abs. 1), andererseits erlaubt derselbe Artikel die Verarbeitung der Daten entweder bei einer ausdrücklichen Einwilligung des Betroffenen oder für Zwecke der Gesundheitsvorsorge oder etwa „zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren" (Art. 9 Abs. 2 (a), (h) und (i)). Damit ist die Verarbeitung aber nicht pauschal erlaubt, sondern nur unter den sonstigen strengen Voraussetzungen der DSGVO[7]. Das bedeutet aber vor allem, dass die Grundsätze des Datenschutzes aus Art. 6 bestehen und hiernach der Vorrang der informierten Einwilligung des Betroffenen (Art. 6 Abs. 1 Uabs. 1 lit. (a)). Für die Anwendung der Ausnahme gem. (d) „Schutz lebenswichtiger Interessen" besteht im Falle der Pandemie-App wenig Raum, da es sich im Sinne der Richtlinie um eine „unmittelbare Bedrohung" und „konkrete Gefahrensituationen"[8] handeln muss nicht – wie im hier diskutierten Fall – lediglich um die Rückverfolgung von Kontakten mit dem/der Infizierten, die nur mittelbar auf Wahrscheinlichkeitsrechnungen basiert. Eine Verarbeitung ist aber gemäß (e) möglich, wenn sie „für die Wahrnehmung einer Aufgabe erforderlich (ist), die im öffentlichen Interesse liegt". Ähnlich wie bei der ePrivacy-Richtlinie kommen aber auch **Grundsätze des Datenschutzes** zur Geltung: eine informierte Einwilligung mit Widerrufsrecht, strikte Zweckbindung der Verarbeitung und Verwendung (Art. 5 I (b)), Datenminimierung (Art. 5 I (c)), zeitliche Speicherbegrenzung (Art. 5 I (c)).

II. Bisherige datenschutzrelevante App-Lösungen zur COVID-Bekämpfung

Bisher sind folgende Mobilfunk-Daten-Lösungen zum Einsatz gekommen oder in der Diskussion. Sie knüpfen in ihrer Zielsetzung grundsätzlich entweder an die (Rück-)Verfolgung der bisherigen Kontakte von Daten-Emittenten (hier Kontakt-Verfolgung) oder an Verfolgung oder Überwachung ihres Verhaltens an (hier Verhaltens-Verfolgung) an:

a. Kontakt-Verfolgung

i. Bewegungsdaten bei Mobilfunkanbietern

Die Verfolgung der Kontakte würde über die bei Mobilfunkanbietern gespeicherte Zuordnung eines Mobiltelefons zu einem oder mehreren Funktürmen erfolgen, was allerdings grobmaschig wäre: die Position des Gerätes in Städten würde sich auf etwa 150 Meter (Umkreis der Antenne) genau bestimmen lassen, auf dem Land könnte es sich um mehrere Quadratkilometer handeln. Die Idee einer dauerhaften Verpflichtung zur Übermittlung dieser Daten nach Vorschlag des Bundesgesundheitsministers wurde nach starker Kritik wieder fallen gelassen.

ii. Annäherungs-Ortung mittels Bluetooth

Mit Bluetooth als Funktechnologie für den Nahbereich sollen Mobilgeräte untereinander pseudonymisierte Tokens austauschen, wenn ihre Nutzer*innen sich in übertragungsrelevanter Nähe zueinander begegnen. So können relevante Nahkontakte über einen beschränkten Zeitraum zurückverfolgt werden, die bei Infektion einer Kontaktperson informiert werden.

b. Verhaltens-Verfolgung

i. Tracking von Bevölkerungsbewegungen („heat maps")

Verschiedene Mobilfunkanbieter übermittelten im März Datensätze etwa an das Robert-Koch-Institut. Nach Angaben der Anbieter waren die

[7] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, DSGVO Art. 9 Rn 24.
[8] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, DSGVO Art. 6 Rn 62.

Büro Dr. Sergey Lagodinsky MdEP Rue Wiertz 60 ASP 8H255 B - 1047 Brüssel

Tel.: +32 228 459 12 E-Mail: sergey.lagodinsky@europarl.europa.eu

Datensätze über 20 Personen gemittelt und somit anonymisiert, ließen jedoch die Erstellung sogenannter „heat maps" zur Feststellung von Ansammlungen etwa in bestimmten Supermärkten oder an anderen Orten zu.

ii. Massenhafte individuelle Beobachtung/Klassifizierung/Sanktionierung

1. Südkorea
   Neben Massen-Tests der Bevölkerung setzte Südkorea zunächst auf eine Kontaktverfolgung durch eine Kombination von Kameraüberwachung, Handy-Ortungsdaten und Kreditkarten-Transaktionen. Im späteren Verlauf wurden Anwohner*innen über Notfall-Meldungen auf Mobiltelefonen auf Infektionsfälle in der Nachbarschaft hingewiesen, teilweise mit Informationen darüber, welche Nahverkehrsmittel die betroffene Person genutzt hatte, und ob sie einen Mundschutz trug. Darüber hinaus kommen etwa an Gebäude-Eingängen Wärmebildkameras zur Temperaturmessung zum Einsatz.

2. China
   Aufbauend auf bestehenden „Social Credit"-Systemen entwickelte das IT-Unternehmen Alibaba die „Alipay Health Code"-App, die zur Einschätzung des individuellen Risiko-/Infektionsstatus für die Bevölkerung verpflichtend wurde. Für den Zugang etwa zum öffentlichen Nahverkehr ist das Vorzeigen der App, die mit einem Ampel-System und einem QR-Code den Status der Person anzeigt, notwendig. Es wird berichtet, dass Bewegungsdaten der Polizei zugänglich gemacht werden. Auch Berichte über fehlerhafte „rote" Einstufungen wurden bekannt, wonach es den Personen nicht mehr möglich war, etwa zur Arbeit oder nach Hause zu gelangen.

iii. Beobachtung individuellen Isolierungszwangs
Bürger*innen in Quarantäne müssen in Südkorea eine GPS-Tracking-App herunterladen, also eine Art elektronische Fußfessel. Bei Verstößen gegen Quarantänebestimmungen können Strafen von umgerechnet über 2000€ verhängt werden. Russland arbeitete Berichten zufolge an einer ähnlichen Anwendung.

III. Rechtliche und politische Bewertung

Vor dem Hintergrund der obigen Rechtsgrundsätze und im Kontext der gegenwärtigen Situation komme ich zur folgenden rechtlichen und politischen Bewertung der vorhandenen App-Lösungen:

a. Massenhafte Verhaltens-Verfolgung: unrechtmäßig

Aufgrund des Grundsatzes der Verhältnismäßigkeit und anderer grundrechtlicher Prinzipien sind Lösungen, die im großen Stil Verhalten der Bürger*innen verfolgen, grundsätzlich abzulehnen. Dies gilt umso mehr angesichts der bisher glücklicherweise überschaubaren Pandemie-Statistik und einem meist nicht unmittelbar auf den jeweiligen Daten-Emittenten zurückführbaren Risiko-Potential. Eine massenhafte Verhaltensdurchsetzung und Verhaltensbeobachtung ist nicht möglich, da dies in der derzeitigen Situation insbesondere die Grenzen von Art. 52 der Europäischen Grundrechte-Charta sowie (schon der Natur eines Zwangs nach) den Grundsätzen der Einwilligung sowie der Datenminimierung widersprechen würde.

b. Individuelle Verhaltens-Verfolgung: unverhältnismäßig

Büro Dr. Sergey Lagodinsky MdEP Rue Wiertz 60 ASP 8H255 B - 1047 Brüssel

Tel.: +32 228 459 12 E-Mail: sergey.lagodinsky@europarl.europa.eu

Zu denken wäre allenfalls an eine individuelle Verhaltensbeobachtung bei Isolationszwang. Hier bestimmt § 30 InfSG sehr weitgehende, auch zum Teil in den Datenschutz hinein eingreifende Maßnahmen, die ausdrücklich als zulässige Eingriffe in Grundrechte, auch wohl in das Recht auf informationelle Selbstbestimmung, proklamiert werden. Jedoch muss auch an dieser Stelle nach Grundsätzen der Verhältnismäßigkeit verfahren werden und die genaue Ausgestaltung einer solchen (bisher hypothetischen) App beobachtet und evaluiert werden. Insbesondere wäre darauf zu achten, dass die Datenschutzstandards für Infizierte nicht unter diejenigen für Strafgefangenen fallen. Auch an einer datenschutzrechtlichen Gleichstellung bzw. Schlechterstellung gegenüber Strafgefangenen (etwa nach entsprechendem Landesrecht) würde Geeignetheit und Angemessenheit der Maßnahmen und somit auch ihre Verhältnismäßigkeit scheitern.

c. **Tracking von Bevölkerungsbewegungen: bedingt zulässig**

Nach der Übermittlung von Bewegungsdaten von Mobilfunkanbietern an Seuchenbekämpfungsbehörden in verschiedenen Mitgliedsländern der EU ist nach dem öffentlichen Bekunden der Beteiligten davon auszugehen, dass es sich um anonymisierte und gemittelte Daten handelt, die also nicht zur Erstellung individueller Bewegungsprofile geeignet sind, und keine Rückschlüsse auf die betroffenen Personen zulassen. Die sogenannten „heat maps" sollen allenfalls die Effektivität der Abstands-Anordnungen evaluierbar machen, und eine Reaktion auf eventuelle Bewegungen von Personen aus Corona-Hotspots heraus ermöglichen.
In jedem Fall muss durch eine klare Zweckbindung durch Regulierungsbehörden deutlich gemacht werden, dass die Daten nicht zu Zwecken der Kontrolle und Lenkung von Menschen in Gruppen („crowd control") verwendet werden dürfen.

d. **Dezentrale individuelle Kontakt-Verfolgung: zulässig und zielführend unter Bedingungen**

Die Ansätze zur Kontakt-Verfolgung sind im Gegensatz zur Verhaltens-Verfolgung weniger invasiv, müssen aber ihrerseits datenschutzkonform sein.

Die in Frage stehende Bluetooth-Lösung müsste insbesondere nach folgenden Prinzipien funktionieren, damit die Nutzung rechtlich und politisch unbedenklich ist:

i. Prinzip der **effektiven Freiwilligkeit**. Wichtig wäre etwa insbesondere:
   - dass die App-Nutzer*innen vor (!) der Installation erschöpfende und in einfacher Sprache gefasste Informationen über die Zwecke der Datenerhebung und -verarbeitung erhalten, über eigene Rechte sowie über die Möglichkeit der Unterbrechung der Nutzung aufgeklärt werden;
   - dass die Entscheidung zur Installation der App nicht mit staatlich sanktionierten Benachteiligungen aber auch nicht mit staatlich sanktionierten Bevorteilungen aus ähnlichen oder nicht verwandten Gebieten einhergeht;
   - dass die Nutzung der App mit keiner öffentlicher Kennzeichnung/Sichtbarwerdung der Nutzung einhergeht, um sozialen Druck zur Nutzung zu vermeiden;
   - dass ein Ausstieg aus der Nutzung der App jederzeit, mit sofortiger Wirkung möglich ist. Ein Ausstieg wäre insbesondere dann effektiv möglich, wenn die Applikation dezentral konzipiert ist, eine Datenspeicherung also nur auf dem Endgerät stattfände, nicht etwa auf einem zentralen Server.

ii. Prinzip der **strikten Zweckbindung**:

Büro Dr. Sergey Lagodinsky MdEP Rue Wiertz 60 ASP 8H255 B - 1047 Brüssel

Tel.: +32 228 459 12 E-Mail: sergey.lagodinsky@europarl.europa.eu

- Die gesammelten Daten müssen nach Möglichkeit schon technisch ausschließlich dem Zweck der Kontakt-Verfolgung vorbehalten sein. Eine Umwidmung der Datennutzung sollte auch zu den nach DSGVO vorgesehenen Ausnahmezwecken (Art. 6 Abs 4 iVm Art. 23 DSGVO) sowie nach erfolgter Einwilligung des Betroffenen nicht möglich sein, um den Anschein und Sorgen vor Missbrauch durch staatliche oder sonstige Stellen entgegenzuwirken. Auch zu diesem Zweck wäre eine dezentrale Speicherungslösung förderlich.

iii. Prinzip der **Datenminimierung und Speicherbegrenzung**:

- Die Sammlung der Daten muss zeitlich begrenzt (etwa auf den durchschnittlichen Zeitraum der Feststellung einer Infektion beschränkt oder bis zu 14 Tage lang) sein, anschließend sollten die Daten gelöscht werden.
- Auch dieses Prinzip wird am stärksten durch die Auslösung der Löschung der Daten auf dem Endgerät des Nutzers gewährleistet, da sie somit den Privatbereich des Nutzers nicht verlassen und die Löschung nicht etwa erst durch einen zentralen Server ausgelöst werden muss.

iv. Prinzip der **Dezentralisierung**:

- Wie oben dargestellt ist die beste Gewähr für eine legale und effektive Erhebung, Speicherung und Verarbeitung der Daten deren dezentrale Handhabung. Auch wenn Dezentralisierung keine direkte rechtliche Anforderung ist, ist sie in diesem Falle der Weg, der die Umsetzung der meisten Prinzipien des Datenschutzes sichert und erst ermöglicht. Insbesondere gemäß dem Prinzip des „absolut Nötigen" ist gedient, wenn eine dezentrale Lösung möglich und mindestens annähernd genauso effektiv wie eine Lösung mit zentraler Speicherung ist. Darüber hinaus entsteht durch dezentrale Speicherung eine geringere Vulnerabilität für Hackerangriffe Dritter, da es einem Angreifer nicht mehr möglich ist, alle oder einen Großteil der Daten mit einem einzelnen Angriff zu erhalten.

v. Prinzip der **ganzheitlichen Betrachtung**:

- Eine technisch mögliche und rechtlich zulässige Lösung kann nur sinnvoll sein, wenn ihre Auswirkungen auch sozial und psychologisch verträglich sind. Sollten Kontaktpersonen über eine mögliche Infektion informiert werden, muss seitens der staatlichen Stellen klar gemacht werden, welche Konsequenzen sozial und arbeitsrechtlich daraus resultieren. Es bringt wenig, gerade in der Situation einer Krise, Menschen allein mit solchen Informationen zu lassen. Geklärt muss etwa werden, ob und wo realistische Testmöglichkeiten bestehen, inwiefern ein Negativtest die Notwendigkeit einer Selbstquarantäne beseitigt oder eine solche weiterhin empfohlen bleibt, wie die Versorgung der Familien und Kinder in einem solchen Fall funktioniert, ob ein Anspruch der betroffenen Arbeitnehmer*innen auf Fernarbeit besteht bzw. welche Rechte im Falle einer Unmöglichkeit von „Home-Office" bestehen, etwa ob eine Krankschreibung zulässig ist. Ggf. müsste auch eine Möglichkeit für eine psychologische Betreuung oder niedrigschwellige medizinische Beratung bestehen. Es muss klar sein, dass dank dieser Applikation viel mehr Menschen von einer vagen Risiko-Benachrichtigung betroffen sind und klare rechtliche und soziale Informationen brauchen. Die Evaluation und Klärung der sozialen und psychologischen Auswirkungen der Applikation

Büro Dr. Sergey Lagodinsky MdEP Rue Wiertz 60 ASP 8H255 B - 1047 Brüssel

Tel.: +32 228 459 12 E-Mail: sergey.lagodinsky@europarl.europa.eu

müssen von den staatlichen Stellen vor (!) der Einführung der technischen Lösung erfolgen.

Ergebnis: Tracking von Bevölkerungsbewegungen ist nur unter strenger Einhaltung der Zweckbindung der Datenverwendung zulässig. Individuelle Kontakt-Verfolgung per App (Bluetooth-Lösung) soll nur dezentral, freiwillig, zweckgebunden und befristet erfolgen. Darüber hinaus muss eine vorbeugende Regulierung von psychologischen, arbeitsrechtlichen und sozialen Auswirkungen einer solchen App-Verwendung erfolgen.

Anhang:

- Stellungnahme der Europäischen Kommission: Empfehlung zur Unterstützung von Ausstiegsstrategien durch Daten von mobilen Geräten und Mobil-Apps https://ec.europa.eu/commission/presscorner/detail/de/ip_20_626

- Stellungnahme des EU-Datenschutzausschusses: https://edpb.europa.eu/news/news/2020/european-data-protection-board-issue-guidance-data-processing-fight-against-covid-19_de

- Stellungnahme des Helmholtz-Zentrum für Informationssicherheit zum Ausstieg aus dem PEPP-PT-Konsortium und zur Unterstützung des dezentralen Ansatzes des DP-3T-Projekts: https://cispa.saarland/de/2020/04/20/contact-tracing-app-for-the-sars-cov-2-pandemic.html

Büro Dr. Sergey Lagodinsky MdEP Rue Wiertz 60 ASP 8H255 B - 1047 Brüssel

Tel.: +32 228 459 12 E-Mail: sergey.lagodinsky@europarl.europa.eu