SH Schleswig-Holstein
Ministerium für Inneres,
ländliche Räume
und Integration

MUT VERBINDET
TAG DER DEUTSCHEN EINHEIT
KIEL – 2./3. OKTOBER 2019

Ministerium für Inneres, ländliche Räume und Integration
Postfach 71 25 | 24171 Kiel

An den
Vorsitzenden des Finanzausschusses
des Schleswig-Holsteinischen Landtages
Herrn Thomas Rother, MdL
Landeshaus
24105 Kiel

nachrichtlich:
Frau Präsidentin
des Landesrechnungshofs
Schleswig-Holstein
Dr. Gaby Schäfer
Berliner Platz 2
24103 Kiel

über das:
Finanzministerium
des Landes Schleswig-Holstein
Düsternbrooker Weg 64
24105 Kiel

Schleswig-Holsteinischer Landtag
Umdruck 19/2466

Staatssekretär

gesehen
und weitergeleitet
Kiel, den 15.Mai 2019
Silke Schneider

7. Mai 2019

Mein Zeichen: 25953/2019

Information des Finanzausschusses über die Kooperationsvereinbarung zur „Dienstleistungsvereinbarung über Bereitstellung, Betrieb und Kostenverteilung eines zentralen Einsatzkommunikations- und Unterstützungssystems (EKUS) für die Spezialeinheiten der Länder und des Bundes“

Sehr geehrter Herr Vorsitzender,

ich möchte Sie darüber unterrichten, dass das Ministerium für Inneres, ländliche Räume und Integration der Kooperationsvereinbarung zur „Dienstleistungsvereinbarung über Bereitstellung, Betrieb und Kostenverteilung eines zentralen Einsatzkommunikations- und Unterstützungssystems (EKUS) für die Spezialeinheiten der Länder und des Bundes“ beitreten wird. Die Entwürfe der Dienstleistungsvereinbarung und der Kooperationsvereinbarung sind beigefügt.

Vor dem Hintergrund der terroristischen Anschläge von Paris, Kopenhagen und Brüssel sowie der Gefährdungslage angesichts der Rückkehrer aus islamistischen Krisengebieten sieht es der AK II als erforderlich an, für die Spezialeinheiten der Länder und des Bundes ein länderübergreifendes und einheitliches Einsatz-Kommunikations- und Unterstützungs-System (EKUS) auf gesicherten Endgeräten einzuführen (Beschluss des AK II in der 248.

Sitzung vom 13./14.04.2016). EKUS ist ein System, welches die Funktionalitäten eines Polizei-Messengers mit digitalen Kartendiensten, Offline-Verfügbarkeiten von Einsatzdaten auf den Endgeräten der Einsatzkräfte sowie Befehlsstellenfunktionalitäten verbindet. Eine Zusammenarbeit der Spezialeinheiten des Bundes und der Länder im Kontext der Terrorismusbekämpfung und herausragender Lagen mit Besonderer-Aufbau-Organisation (BAO-Lagen) ist unumgänglich.

Mit Beschluss des AK II (255. Sitzung vom 11.04.2018) wurde das Bundeskriminalamt (BKA) beauftragt, als zentraler IT-Dienstleister eine bundeseinheitliche Lösung auf der Grundlage der Software „SE-Netz“ („Spezialeinheiten-Netz“ entwickelt vom Landeskriminalamt (LKA) Sachsen in Kooperation mit dem Fraunhofer Institut für Verkehrs- und Infrastruktursysteme) bereitzustellen und zu betreiben.

Eine zwischen dem LKA Sachsen und dem Fraunhofer Institut geschlossene Kooperationsvereinbarung ermöglicht den EKUS-Teilnehmern durch Beitritt zur Kooperationsvereinbarung die Beschaffung der für die Software notwendigen Lizenzen.

Das BKA hat die Dienstleistungsvereinbarung über Bereitstellung, Betrieb und Kostenverteilung eines zentralen Einsatzkommunikations- und Unterstützungssystems (EKUS) für die Spezialeinheiten der Länder und des Bundes erarbeitet, die zwischen dem BKA als zentralem Dienstleister und den EKUS-Teilnehmern abgeschlossen werden soll. Inhalt der Dienstleistungsvereinbarung sind u.a. das Service-Angebot des BKA als zentraler Dienstleister, die Verpflichtungen der EKUS-Teilnehmer sowie die Aufteilung der Kosten.

Zeitplan

Das BKA plant ab Juli 2019 in den Produktiv-Betrieb zu gehen. Voraussetzung ist der Beitritt der EKUS-Teilnehmerländer zu der Kooperationsvereinbarung zwischen dem LKA Sachsen und dem Fraunhofer Institut. Erst wenn der Beitritt aller EKUS-Teilnehmer erfolgt ist, beginnt der Produktiv-Betrieb.

Kosten

Die Kosten für die Bereitstellung und den Betrieb von EKUS werden nach dem modifizierten Königsteiner Schlüssel auf alle Beteiligten umgelegt.

Auf der Grundlage der bis zum 30.06.2019 gültigen Preisliste sind verschiedene Lizenzstufen hinterlegt. Für das LKA Schleswig-Holstein würde ein Basispaket für bis zu 300 Nutzer ausreichend sein. Kosten dafür liegen bei 95.200 Euro.

Kosten für die Systempflege für die Jahre 2019 – 2025 durch das Fraunhofer Institut werden im Rahmen des modifizierten Königsteiner Schlüssels (zz. bei ca. 2,8%) auf die Länder und den Bund umgelegt. Gesamtkosten nach Abzug von Lizenzeinnahmen belaufen sich auf ca. 1.900.000 Euro, Anteil SH in 2019 beträgt ca. 53.200 Euro.

Die Gesamtkosten für die Beschaffung der Hardware-Infrastruktur werden durch das BKA mit 1.601.000 Euro, für den Betrieb 2020 mit 1.403.000 Euro und für den weiteren Betrieb ab 2021 mit ca. 1.743.000 Euro angegeben. Schleswig-Holsteins Anteil wird nach dem

modifizierten Königsteiner Schlüssel berechnet. Die erstmaligen Kosten werden vom BKA vorfinanziert und anschließend von den EKUS-Teilnehmern zurückgefordert.

Kosten in 2019: 148.500 Euro (Lizenzen und Support für die Jahre 2019 – 2025)
Kosten in 2020: 84.000 Euro (Hardwareinfrastruktur inkl. Rückforderung BKA aus 2019)
Kosten ab 2021: 49.000 Euro (Hardwareinfrastruktur)

Die Haushaltsmittel zur Finanzierung der Vereinbarung sind im IT-Haushalt (Einzelplan14) eingeplant. Das ZIT SH hat diese Vorlage mitgezeichnet.

Mit freundlichen Grüßen

gez. Torsten Geerdts

Anlagen: 01_Anlage_Entwurf_Dienstleistungsvereinbarung
02_Anlage_Entwurf_Kooperationsvereinbarung

Dienstleistungsvereinbarung

über Bereitstellung, Betrieb und Kostenverteilung

eines

zentralen Einsatzkommunikations- und Unterstützungssystems

(EKUS)

für die Spezialeinheiten der deutschen Polizeien

und der

Zollverwaltung

zwischen

der Bundesrepublik Deutschland,

vertreten durch das
Bundesministerium des Innern, für Bau und Heimat

dieses vertreten durch das
Bundeskriminalamt, (zentraler Dienstleister)
Thaerstraße 11, 65173 Wiesbaden

und

den nachfolgend aufgeführten Vertragspartnern (EKUS-Teilnehmer)
[1. vertragsschließende Behörde BB]
[2. vertragsschließende Behörde BE]
[3. vertragsschließende Behörde BW]
[4. vertragsschließende Behörde BY]
[5. vertragsschließende Behörde HB]
[6. vertragsschließende Behörde HE]
[7. vertragsschließende Behörde HH]
[8. vertragsschließende Behörde MV]
[9. vertragsschließende Behörde NW][10.

vertragsschließende Behörde NI]
[11. vertragsschließende Behörde RP]
[12. vertragsschließende Behörde SH]
[13. vertragsschließende Behörde SL]
[14. vertragsschließende Behörde SN]
[15. vertragsschließende Behörde ST]
[16. vertragsschließende Behörde TH]
[17. vertragsschließende Behörde BPOL]
[18. vertragsschließende Behörde ZOLL]

(BKA und Vertragspartner zusammen
nachfolgend als „Beteiligte“ bezeichnet)

Version 0.85 Stand: 13.03.2019

Inhaltsverzeichnis

§ 1. Gegenstand der Vereinbarung

Der zentrale Dienstleister richtet ab xx.xx.2019 einen IT-Service EKUS in Form einer einheitlichen, zentral in den Rechenzentren des BKA betriebenen Softwarelösung ein, um den Spezialkräften des Bundes und der Länder eine Einsatzunterstützung sowohl bei Verwendung gesicherter mobiler Endgeräte als auch bei Nutzung ortsfester Büroarbeitsplätze zu ermöglichen.

Kommentar [HM1]: Wird nachgetragen sobald die DLV abgestimmt ist

Das BKA übernimmt die Verantwortung für die Bereitstellung und den Betrieb der Zentralanwendung und hat damit die Aufgabe, eventuell notwendige technische und betriebliche Ertüchtigungs-, Anpassungs-, Modernisierungs- und Erweiterungsmaßnahmen federführend umzusetzen.

Weiterhin erbringt das BKA im Rahmen der von den EKUS-Teilnehmern gemeinsam finanzierten Dienstleistungskapazitäten Unterstützungsleistungen zur Sicherstellung eines reibungslosen und anforderungsgerechten Betriebs der EKUS Zentralinstanz.

Die Unterstützung im Bereich mobile Endgeräte beschränkt sich auf die Bereitstellung einer mobilen Anwendung (App). Die Lieferung sicherer mobiler Endgeräte sowie die Bereitstellung einer IT-Infrastruktur für den Betrieb und die Verwaltung mobiler Endgeräte sind nicht Gegenstand dieser Vereinbarung. Gleiches gilt für Beratungs- und Unterstützungsleistungen im Bereich mobiler Endgeräte.

Diese Vereinbarung regelt die vom zentralen Dienstleister zu erbringenden Leistungen, die Mitwirkungspflichten der EKUS-Teilnehmer und die Modalitäten der Kostenverrechnung zwischen den Vertragspartnern.

.

§ 2. EKUS-Nutzergremium

Die gemäß Beschluss des UA IuK vom 16.01.2018 (33. Sondersitzung in Wiesbaden) einberufene und von den Gremien AG Kripo, UA FEK und UA IuK gemeinsam mandatierte Expertengruppe EKUS ist, wie vom BKA mit Schreiben vom 11.07.2018 erbeten, von den EKUS-Teilnehmern um technische Expertise erweitert worden. Gleichzeitig wurde das erweiterte Gremium auf Dauer als EKUS-Nutzergremium im Sinne des Berichts, den das BKA dem AK II auf seiner 255. Sitzung am 11./12.04.2018 in Wiesbaden zur Realisierung von EKUS auf Basis von SE-Netz 2.0 vorgelegt hat, mandatiert.

Dieses Gremium legt sowohl fachlichen als auch technischen Weiterentwicklungsbedarf fest und priorisiert ihn. Die Sitzungen des Gremiums werden unter Federführung des BKA in enger Zusammenarbeit gemeinsam vom BKA, einer beim LKA Sachsen eingerichteten EKUS-Geschäftsstelle und dem Fraunhofer-Institut für Verkehrs- und Infrastruktursysteme (Fh-IVI) vorbereitet und durchgeführt.

Jeder Beteiligte hat eine Stimme, entsendet aber zwei Vertreter in das Gremium, um sowohl technische als auch die fachliche Aspekte abdecken zu können. Für das Zustandekommen eines Beschlusses ist eine 2/3-Merheit erforderlich. Können sich die beiden Vertreter eines Beteiligten nicht auf ein Votum einigen, wird das als Enthaltung gewertet. An Beschlüsse des Gremiums ist der zentrale Dienstleister dann nicht gebunden, wenn die Umsetzung einen unvertretbar hohen Aufwand erfordert oder zu nicht vertretbaren Betriebs- oder Sicherheitsrisiken führen würde.

Vom Gremium verabschiedete Anforderungen stellen gemeinsame Anforderungen aller EKUS-Teilnehmer dar und werden daher auch von allen Teilnehmern gemeinsam finanziert.

§ 3. EKUS-Forschungskooperation

Grundlage von EKUS ist die Software SE-Netz 2.0, die im Rahmen einer Forschungs- und Entwicklungskooperation (F&E-Kooperation) zwischen dem LKA Sachsen und dem Fh-IVI realisiert worden ist. Die Softwareentwicklung erfolgte durch das Fh-IVI. Diese F&E-Kooperation wird mit dem Ziel der Bereitstellung und fortlaufenden Verbesserung des bundesweit gemeinsam genutzten EKUS bis 31.12.2025 fortgeführt. Im Rahmen der Neuausrichtung hat das BKA die Federführung der Forschungskooperation vom LKA Sachsen übernommen.

Die Softwareentwicklung innerhalb der F&E-Kooperation wird aus den Lizenzeinnahmen und über einen federführend vom BKA geschlossenen Weiterentwicklungsvertrag, dessen Kosten auf die EKUS-Teilnehmer umgelegt werden, finanziert. Die operative Steuerung der gemäß §2 vom Nutzergremium festgelegten Aufgaben der F&E-Kooperation übernimmt die EKUS-Geschäftsstelle beim LKA Sachsen.

Im Bereich Softwarepflege und -weiterentwicklung werden die von den EKUS-Teilnehmern im Umlageverfahren gemeinsam finanzierten Aufgaben der F&E-Kooperation vom EKUS-Nutzergremium (vgl. §2) definiert und priorisiert. Da es sich bei EKUS um ein F&E-Projekt handelt, kann eine vollständige und zeitgerechte Umsetzung dieser Anforderungen durch das Fh-IVI nicht garantiert werden. Bei der vom BKA bereitgestellten EKUS-Software handelt es sich um vom Fh-IVI im Rahmen der F&E-Kooperation realisierte und offiziell freigegebene Software-Releases.

Voraussetzung für die Nutzung der EKUS-Software sind die Mitgliedschaft in der EKUS-F&E-Kooperation und der Erwerb einer ausreichenden Zahl von EKUS-Nutzerlizenzen. Diese Voraussetzungen sind von den EKUS-Teilnehmern vor Nutzung der zentralen EKUS-Instanz in eigener Zuständigkeit und auf eigene Kosten zu schaffen. Ansprechpartner ist das Fh-IVI. Die Einnahmen aus dem Lizenzverkauf, die das Fh-IVI während der Laufzeit dieses Vertrags mit der EKUS Software erzielt, kann es unter Beachtung der Zweckbindung (§4.1 der KoopV) und unter Einbeziehung der Anwender eigenständig für gezielte F&E-Arbeiten zur Innovation und Zukunftssicherung des Systems einsetzen.

§ 4. Bereitstellung der EKUS-Software

Gemäß Beschluss des AK II auf seiner 255. Sitzung am 11./12.04.2018 wird EKUS auf Basis des Produkts SE-Netz 2.0 des Fh-IVI zur Verfügung gestellt. Das BKA übernimmt hierbei die Rolle eines zentralen Dienstleisters, dessen Aufgabe die zentrale Bereitstellung und der zentrale Betrieb des bundesweit gemeinsam genutzten EKUS (Anwendung inkl. Datenbestand) umfasst.

Die fachlichen Leistungsmerkmale der ersten bereitgestellten EKUS-Version entsprechen denen der Version SE-Netz 2.0. Auch die technischen Leistungsmerkmale sind weitestgehend identisch, Anpassungen werden nur insoweit vorgenommen wie es zur Herstellung der Betriebsfähigkeit in der IT-Infrastruktur des BKA zwingend erforderlich sind. Die Weiterentwicklung der Software ist in §5 geregelt.

Folgende vom Fh-IVI entwickelten EKUS-Software-Komponenten werden zur Nutzung bereitgestellt:

- eine EKUS-App zur Nutzung auf sicheren mobilen Endgeräten (verfügbar für Android und iOS)

- eine browserbasierte EKUS-Kommandooberfläche, verfügbar in mehreren Formfaktoren für die Nutzung auf browserfähigen Endgeräten (u.a. Tablet und PC)
- ein zentral zu betreibendes EKUS-Backend, dessen Hauptaufgabe die sichere Datenhaltung ist.

Darüber hinaus stellt der zentrale Dienstleister die von der EKUS-Software benötigten Basisdienste (z.B. Geodatendienste) zur Verfügung (siehe §7).

Gemäß AK II-Beschluss (248. Sitzung am 13./14.04.2016) haben die EKUS-Teilnehmer die Möglichkeit, in ihrem Zuständigkeitsbereich eine lokale EKUS-Instanz zur Abwicklung landesinterner Einsätze zu betreiben. Implementierung, Betrieb und Support solcher lokaler Instanzen gehören ebenso wie zugehörige weitergehende Unterstützungsleistungen (z.B. Störungsanalyse) nicht zu den Aufgaben des zentralen Dienstleisters. Die Betriebs- und Finanzverantwortung für lokale Instanzen liegt allein beim jeweiligen EKUS-Teilnehmer.

§ 5. Weiterentwicklung der EKUS-Software

Über die polizeifachliche und technische Weiterentwicklung der EKUS-Software entscheidet das EKUS-Nutzergremium (vgl. §2).

Vorschläge der EKUS-Teilnehmer, die innerhalb des Nutzergremiums nicht die erforderliche Mehrheit gefunden haben, werden nicht im Rahmen der gemeinsamen EKUS-F&E-Kooperation realisiert. Der zentrale Dienstleister ist im Rahmen seines in §2 geregelten Vetorechts bei technischem Weiterentwicklungsbedarf, der aus betrieblichen Gründen unabweisbar ist, nicht an ein ablehnendes Votum des Gremiums gebunden. Dieses Recht ist zur Wahrnehmung der Betriebsverantwortung zwingend notwendig.

§ 6. Spezifische Anforderungen einzelner Vertragspartner

EKUS-Teilnehmer und Gruppen von EKUS-Teilnehmern können die Erfüllung von Anforderungen, für die sie im Kreise des EKUS-Nutzergremiums keine ausreichende Mehrheit gefunden haben mit Kenntnisnahme der EKUS-Geschäftsstelle und des zentralen Dienstleisters als zusätzliche, von der Forschungskooperation nicht abgedeckte Aufgaben beim Fh-IVI beauftragen. Voraussetzung ist, dass das Fh-IVI für die Bearbeitung der Zusatzaufträge auf freie Kapazitäten außerhalb der F&E-Kooperation zurückgreifen kann, so dass sich keine negativen Auswirkungen auf die Aufgabenerledigung innerhalb der F&E-Kooperation ergeben. Die Kosten für Zusatzaufträge sind von dem/den jeweiligen Bedarfsträger(n) zu tragen.

Das in §2 formulierte Vetorecht des zentralen IT-Dienstleister gegen Änderungen der EKUS-Software, die unverhältnismäßigen betrieblichen Aufwand verursachen oder die Betriebssicherheit gefährden, gilt auch bezüglich der Umsetzung von Zusatzaufträgen, die außerhalb der F&E-Kooperation realisiert werden sollen.

Mitglieder der EKUS-F&E-Kooperation, die keine EKUS-Teilnehmer sind, haben keine Möglichkeit, in Zusammenhang mit der EKUS-Software Forschungsaufgaben zu beauftragen, die nicht im Einklang mit den Beschlüssen des EKUS-Nutzergremiums umgesetzt werden können.

§ 7. Datenspeicherung

Innerhalb des EKUS werden

- Einsatzdaten der polizeilichen Spezialeinheiten,
- Daten zu Organisationstruktur und Personal polizeilicher Spezialeinheiten,
- Daten aus gesetzlich vorgeschriebener Protokollierung und
- Daten, die aus technischen oder sicherheitstechnischen Gründen (z.B. für Fehler- und Bedrohungsanalyse) protokolliert werden,

gespeichert. Dazu gehören auch personenbezogene Daten von Personen, die bei polizeilichen Einsätzen eine Rolle spielen. Protokolldaten werden nur temporär gespeichert und in einen zentralen Protokollserver überführt.

Die Datenspeicherung erfolgt in den Rechenzentren des zentralen Dienstleisters. Er ist verpflichtet, in ausreichendem Umfang Speicherplatz und Rechenleistung zur Verfügung zu stellen sowie geeignete Maßnahmen gegen unbefugten Zutritt, Datenverlust und unberechtigte Datenveränderungen durch das Betriebspersonal zu implementieren. Zugriffsberechtigt sind EKUS-Nutzer im Rahmen des EKUS-Berechtigungskonzepts, die jeweils zuständigen Datenschutz- und Geheimschutzbeauftragten sowie das vom zentralen Dienstleister für den EKUS-Betrieb eingesetzte Personal.

Zugriffe Dritter auf EKUS sind grundsätzlich nicht zulässig. Sofern externe Firmen zur Erfüllung der ihnen vom zentralen Dienstleister übertragenen Aufgaben unabdingbar EKUS-relevante Informationen und/oder in EKUS gespeicherte Informationen benötigen, werden mit diesen Firmen Vereinbarungen zu Datenschutz, Geheimhaltung und Informationssicherheit abgeschlossen bevor diesen die Informationen bereitgestellt werden.

Weiteres regelt §11 der Vereinbarung zur Auftragsdatenverarbeitung im Rahmen von EKUS.

§ 8. Sonstige Services

Ergänzend zu den EKUS-Kernfunktionalitäten werden folgende Services bereitgestellt:

- IT-Infrastruktur

  Der zentrale Dienstleister verfügt über eine IT-Infrastruktur, deren Eignung für den Betrieb von polizeilichen IT-Anwendungen, die gemeinsam von Bundes- und Landesdienststellen genutzt werden und hohe bis sehr hohe Anforderungen in den Bereichen Datenschutz, Datensicherheit und Verfügbarkeit haben, durch langjährige Praxis nachgewiesen ist. Innerhalb dieser Infrastruktur werden für EKUS die benötigten Ressourcen bereitgestellt. Querschnittliche Rechenzentrumsdienste (RZ-Dienste) wie etwa Backup, Betriebsüberwachung und Netzwerkkonnektivität werden anwendungsübergreifend zur Verfügung gestellt.

- User Help Desk

  Der zentrale Dienstleister betreibt anwendungsübergreifend einen zentralen User Help Desk, der 7*24h für Störungsmeldungen zu EKUS zur Verfügung steht. Dieser User Help

Desk wird in der Regel von der IT-Serviceorganisation der Teilnehmer angesprochen und nicht von dessen Endnutzern.

- Bereitstellung einer Standardausstattung an digitalen Karten und Geoinformationen

  Der zentrale Dienstleister betreibt einen zentralen Geoinformationsserver, auf dem ein Grunddatenbestand, der mindestens Deutschland abdeckt, bereitgestellt wird. Die Informationen stehen allen Teilnehmern über eine vom zentralen Dienstleister festgelegte Standardschnittstelle 7*24h zur Verfügung. Ein Download von Informationen zur Offline-Nutzung durch EKUS-App und -Kommandooberfläche ist möglich.

- Bereitstellung teilnehmerspezifischer Karten- und Geodaten

  Der zentrale Dienstleister ist bereit, Geoinformationen, die von den Teilnehmern in einem vom zentralen Geoinformationsserver unterstützten Format zur unentgeltlichen Nutzung durch alle Teilnehmer bereit gestellt werden, über den zentralen Kartenserver bundesweit verfügbar zu machen, sofern der dadurch entstehende Mehraufwand auf die EKUS-Teilnehmer umgelegt werden kann und sich durch die Bereitstellung keine negativen Auswirkungen auf andere den zentralen Kartenserver nutzende Anwendungen ergibt. Die konkreten Rahmenbedingungen werden durch den zentralen Dienstleister in Abstimmung mit dem EKUS-Nutzergremium festgelegt.

- Netzwerkkonnektivität/Bandbereite (CNP)

  Das Hauptträgernetz der Kommunikation zwischen EKUS-Endgeräten und dem EKUS-Backend ist das Corporate Network der Deutschen Polizei (CNP), obere und untere Netzebene. Die etablierten Prozesse zur bundesweiten Sicherstellung der Netzkonnektivität und ausreichender Bandbreiten im CNP werden durch EKUS nicht verändert. Der zentrale Dienstleister verpflichtet sich, die von EKUS benötigten Übertragungskapazitäten im CNP/ON zeitgerecht bereit zu stellen.

- Nutzer- und Berechtigungsverwaltung

  Grundlage der Nutzer- und Berechtigungsverwaltung für EKUS soll perspektivisch ein vom zentralen Dienstleister querschnittlich für mehrere Bund-/Länderanwendungen bereitgestelltes zentrales Accessmanagement sein. Bis zur Verfügbarkeit der querschnittlichen Anwendung erhalten die EKUS-Teilnehmer Zugriff auf die SE-Netz interne Nutzer- und Berechtigungsverwaltung. Sie wird von stationären lokalen Arbeitsplätzen erreichbar sein, die über das CNP mit den Rechenzentren des zentralen Dienstleisters verbunden sind. Alternativ können Benutzer- und Berechtigungsdaten über die LDAP-Schnittstelle von EKUS importiert werden.

§ 9. Erreichbarkeit und Verfügbarkeit des EKUS

EKUS ist nur von sicheren mobilen Endgeräten, die im Endgerätemanagement des jeweiligen EKUS-Teilnehmers erfasst und für die Nutzung von EKUS berechtigt worden sind, sowie von Büroarbeitsplätzen im CNP (untere Netzebene) des jeweiligen Vertragspartners erreichbar. Sollten EKUS-Teilnehmer Interesse daran haben, die vom BKA realisierte Anbindung mobiler Endgeräte an das EKUS-Zentralsystem mit zu nutzen, ist das BKA gerne bereit, die technische und finanzielle

Machbarkeit im Einzelfall zu prüfen und im Positivfall ein entsprechendes Dienstleistungsangebot zu machen.

EKUS steht nur authentifizierten Nutzern, die in der zentralen EKUS-Benutzerverwaltung erfasst sind, im Rahmen der dort hinterlegten Rechte zur Verfügung. Bei Verdacht auf missbräuchliche Nutzung von Zugangsdaten kann der Zugang verweigert werden.

Voraussetzung für die Nutzung von EKUS ist eine nach polizeilichen Standards sichere Netzwerkverbindung zu den Rechenzentren des zentralen Dienstleisters. Geht die Netzwerkverbindung verloren, kann die EKUS-App auf mobilen Geräten in eingeschränktem Umfang (sogenannter Offline Modus) weiter genutzt werden.

Die von der EKUS-Anwendung genutzte IT-Infrastruktur in den Rechenzentren des BKA und das Verbindungsnetz (CNP/ON) stehen im 7*24h Betrieb hochverfügbar rund um die Uhr zur Verfügung. Der Betrieb der Anwendung wird permanent überwacht. Im Falle einer Störung, durch die die Nutzung des EKUS nicht mehr möglich bzw. ernsthaft eingeschränkt ist, werden sofortige Maßnahmen zur Störungsanalyse und Wiederherstellung der vollen Funktionsfähigkeit eingeleitet. Aufgrund des vom EKUS-Hersteller angebotenen 5*8 h Supports können Störungen, zu deren Analyse oder Behebung seine Unterstützung erforderlich ist, im ungünstigsten Fall erst zu Beginn des nächsten Werktags bearbeitet werden.

Die Durchführung planbarer Änderungen an der Anwendung oder der genutzten IT-Infrastruktur wird terminlich mit den EKUS-Teilnehmern abgestimmt, sofern eine Unterbrechung oder Beeinträchtigung des EKUS-Betriebs zu erwarten ist.

Der zentrale Dienstleister ist technisch nicht in der Lage, Störungen, die außerhalb seines eigenen Verantwortungsbereichs liegen, zu erkennen und zu beseitigen (siehe auch §10). Aus diesem Grunde kann er keine Mindestverfügbarkeit von EKUS auf den Endgeräten zusichern.

§ 10. Zugriff aus Client-Umgebungen auf EKUS

Die bundesweite Verfügbarkeit von EKUS basiert auf einer IT-Infrastruktur mit bundesweit verteilten Client-Systemen. Die Betriebsverantwortung für die beteiligten IT-Komponenten liegt teilweise beim zentralen Dienstleister und teilweise bei den übrigen EKUS-Teilnehmern. Um die Voraussetzungen eines reibungslosen Betriebs des Gesamtsystems zu schaffen und kontinuierlich aufrecht zu erhalten, ist eine enge Zusammenarbeit aller Teilnehmer erforderlich.

Die EKUS-Teilnehmer übernehmen die Verantwortung für den sicheren Betrieb und die Verfügbarkeit der eigenen Endgeräte und Ortungsserver sowie den lokalen Teil der von EKUS-genutzten Netzinfrastruktur (CNP-UN). Soweit EKUS-relevante IT-Komponenten nicht direkt über das CNP-UN erreichbar sind, ist ein sicherer bidirektionaler Netzübergang in das CNP-UN bereitzustellen.

Der zentrale IT-Dienstleister übernimmt die Verantwortung für den sicheren Betrieb und die Verfügbarkeit des EKUS-Backends, des zentralen Kartenservers, des von EKUS genutzten bundesweiten Verbindungsnetzes (CNP-ON), einschließlich der zugehörigen IT-Infrastruktur, sowie der Import-/Export- und der LDAP-Schnittstelle zum zentralen Backend.

Der zentrale Dienstleister und die EKUS-Teilnehmer verpflichten sich, für den gemeinsamen EKUS-Betrieb folgenden technischen und organisatorischen Unterbau bereit zu stellen:

- Aufbau eines fachlich/technischen Testteams, das in Zusammenarbeit mit dem zentralen Dienstleister alle zur Sicherstellung des Betriebs erforderlichen Tests der Schnittstellen zwischen dem zentralen Backend und der im eigenen Zuständigkeitsbereich liegenden IT-Infrastruktur (einschl. mobiler Endgeräte und Mobil-Infrastruktur) spezifiziert und durchführt. Sofern teilnehmerübergreifende Auswirkungen zu erwarten sind, koordiniert der zentrale Dienstleister die Tests.

- Benennung eines betrieblichen Ansprechpartners, der die übrigen EKUS-Teilnehmer frühzeitig über geplante Änderungen EKUS-relevanter lokaler IT-Komponenten informiert und auf mögliche Auswirkungen hinweist. Sofern teilnehmerübergreifende Auswirkungen zu erwarten sind, wird die geplante Änderung vom zentralen Dienstleister koordiniert.

- 7*24h verfügbare Ansprechstelle (Help Desk) zur Entgegennahme von Störungsmeldungen.

- 7*24h auf Abruf verfügbares geeignetes Personal zur Störungsanalyse und Störungsbeseitigung im eigenen Zuständigkeitsbereich.

- 7*24h Zugriff auf kompetente externe Unterstützung (Supportverträge mit Lieferanten etc.).

Nach Zustimmung durch das EKUS-Nutzergremium können einzelne EKUS-Teilnehmer abweichende interne Regelungen in Bezug auf den 7*24h Betrieb treffen. In diesem Fall kann der zentrale Dienstleister Rückwirkungen auf die bundesweite Verfügbarkeit und Nutzbarkeit des EKUS nicht ausschließen.

Maßnahmen zur Störungsbeseitigung werden vom zentralen Dienstleister koordiniert, solange nicht geklärt ist, in wessen Zuständigkeitsbereich die Störungsursache liegt.

§ 11. Gemeinsame Qualitätssicherung der EKUS-Software

Auf Basis qualitätsgesicherter Releases der EKUS-Software übernimmt der zentrale Dienstleister die Verantwortung für den Bereich der betrieblichen sowie der nichtfunktionalen Anforderungen.

Der zentrale Dienstleister stimmt mit dem EKUS-Nutzergremium, der EKUS-Geschäftsstelle und dem Fh-IVI ab, welche teilnehmerübergreifenden Tests für ein neues EKUS-Software-Release erforderlich sind. Er strebt an, die Gesamtheit aller Tests (polizeifachlich, betrieblich und teilnehmerübergreifend) im Wesentlichen automatisiert durchzuführen.

Weiterhin übernehmen der zentrale Dienstleister und die EKUS-Teilnehmer die Verantwortung für ausreichende Tests der jeweils in ihren eigenen Zuständigkeitsbereich fallenden Komponenten der von EKUS genutzten IT-Infrastruktur und der EKUS-Peripherie (vgl. §10).

Für die Qualitätssicherung der EKUS-App auf den jeweils eingesetzten Endgeräten und unter den jeweiligen Rahmenbedingungen (insbesondere lokale Enterprise Mobility Management Lösung) ist jeder Teilnehmer selbst verantwortlich.

Alle Teilnehmer verpflichten sich zur permanenten Bereitstellung einer Testumgebung für Schnittstellentest, teilnehmerübergreifende Tests und Tests des Gesamtsystems unter Federführung des zentralen Dienstleisters. Der zentrale Dienstleister verpflichtet sich, eine Testumgebung für

fachliche und technische Tests bereitzustellen in der Tests unter wirkbetriebsähnlichen Bedingungen durchführbar sind.

§ 12. Bundesweite Nutzbarkeit von EKUS

Um eine reibungslose Durchführung gemeinsamer Einsätze zu ermöglichen, sind die Vertragspartner gemäß AKII Beschluss (248. Sitzung am 13.4./14.04.2016) verpflichtet, EKUS für alle Einsätze zu nutzen, an denen Spezialkräfte mehrerer Vertragspartner beteiligt sind. Darüber hinaus steht EKUS auch für Einsätze der Vertragspartner zur Verfügung, die vollständig in eigener Zuständigkeit durchgeführt werden.

Auf dem Markt ist eine größere Zahl von mobilen Endgeräte-Ökosystemen verfügbar, die sich technisch teilweise beträchtlich unterscheiden, sodass es nicht möglich ist, EKUS-Apps zu entwickeln, die alle marktgängigen Ökosysteme unterstützen.

Daher legt das EKUS-Nutzergremium verbindlich fest, welche Ökosysteme von den EKUS-Apps zu unterstützen sind. Diese Liste wird entsprechend dem technischen Fortschritt kontinuierlich fortgeschrieben. Es kommen nur Ökosysteme in Frage, die den Mindeststandards für die polizeiliche Nutzung von Smartphones und Tablets als Führungs- und Einsatzmittel der Kommission Architektur und Standards des UA IuK (K-AS) in der jeweils aktuellsten Fassung entsprechen.

Alle EKUS-Teilnehmer verpflichten sich, während der eigenen Nutzungsdauer von EKUS ein oder mehrere mobile Endgeräte-Ökosysteme einzusetzen, die von einem oder mehreren der EKUS-Apps unterstützt werden. Darüber hinaus verpflichten sich alle EKUS-Teilnehmer und der zentrale Dienstleister zu frühzeitigen gemeinsamen Abstimmungen über Änderungs- und Ergänzungsbedarf im Bereich der zu unterstützenden mobilen Endgeräte-Ökosysteme, um daraus resultierenden Anpassungsbedarf bei EKUS frühzeitig erkennen und zeitgerecht beauftragen zu können.

§ 13. Pflichten der EKUS-Teilnehmer

Alle EKUS-Teilnehmer[1] verpflichten sich, in ihrem eigenen Zuständigkeitsbereich

- Vorgaben des Personalrechts (z. B. Beteiligung der Personalvertretungen) und des Haushaltsrechts (z. B. Durchführung von Wirtschaftlichkeitsbetrachtungen) eigenverantwortlich zu erfüllen.
- Test, Qualitätssicherung, Zertifizierung und Freigabe der EKUS-App in Verbindung mit der lokalen sicheren Mobil-Infrastruktur[2] in eigener Zuständigkeit durchzuführen.
- die von EKUS benötigten Übertragungskapazitäten im CNP/UN und in den Transfernetzen der mobilen Kommunikation zeitgerecht bereit zu stellen.[3]

[1] einschließlich des BKA selbst (in der Rolle als EKUS Teilnehmer).

[2] Kombination aus Mobilgerät, gerätespezifischer Sicherheitslösung (z.B. Container) und Mobilgeräte-Management-Lösung (MDM/EMM).

[3] Die erforderlichen Übertragungskapazitäten sind abhängig von der konkreten technischen Umsetzung des EKUS.

- sicherzustellen, dass mobile Endgeräte, von denen aus ein Zugriff auf EKUS möglich ist, nur Personen zur Verfügung stehen, die eine Berechtigung zur EKUS-Nutzung haben.
- eine den EKUS-Sicherheitsanforderungen genügende Nutzerauthentifizierung an mobilen Endgeräten durchzuführen.
- EKUS-Zugang und EKUS-Daten auf einem Mobilgerät unverzüglich zu sperren bzw. zu löschen, wenn der Besitzer des Mobilgeräts seine EKUS-Berechtigung verliert oder das Mobilgerät auf andere Weise in den Besitz einer unberechtigten Person gelangt.
- Stammdaten und spezifische Berechtigungen der EKUS-Nutzer der eigenen Organisation in der EKUS-Nutzer- und Berechtigungsverwaltung (vgl. §7) selbst zu pflegen und fortlaufend aktuell zu halten.
- eine Störungsmeldung an den zentralen Help Desk erst abzusetzen, wenn eine lokale Störung weitestgehend ausgeschlossen worden ist.
- nur Ortungsserver anzubinden, welche die vom zentralen Dienstleister veröffentlichte PAIP-basierte Kommunikationsschnittstelle bereit stellen,
- einen 7*24h-Betrieb der von EKUS mitgenutzten Teile der teilnehmereigenen IT-Infrastruktur sicherzustellen[4],
- bei der Einhaltung teilnehmerspezifischer Sonderregelungen zur IT-Sicherheit und zu den Speicherfristen mitzuwirken.

§ 14. Kostenverteilung

Die tatsächlichen Kosten der Bereitstellung und des Betriebs von EKUS werden nach dem modifizierten Königsteiner Schlüssel auf alle Beteiligten umgelegt (AKII-Beschluss auf der 255. Sitzung am 11./12.04.2018). Der Anteil des Bundes wird zu gleichen Teilen von den beteiligten Bundesbehörden getragen. Diese Gesamtkosten setzen sich zusammen aus:

- den Kosten der initialen EKUS-Beschaffung.
- den Kosten der fortdauernden Aufrechterhaltung der bundesweiten Nutzbarkeit der EKUS-Apps, insbesondere Durchführung notwendiger Anpassungen im Bereich der unterstützten mobile Endgeräte- Ökosysteme nach Vorgaben des EKUS Nutzergremiums.
- den Kosten der funktionalen Weiterentwicklung von EKUS entsprechend der Beschlüsse des EKUS-Nutzergremiums.
- den Kosten der fortlaufenden Anpassung von EKUS an den aktuellen Stand der Technik nach Vorgaben des zentralen Dienstleisters (u.a. Anpassungen an Versionsänderungen der EKUS-Basissoftware).

[4] abweichende Regelungen sind mit Zustimmung des EKUS-Nutzergremiums möglich, vgl. §10.

- den Kosten der SW-Pflege und des Supports auf dem sich aus der Schutzbedarfsanalyse ergebenden Serviceniveau für alle EKUS-Softwarekomponenten, die auf Beschluss des EKUS-Nutzergremiums vom zentralen Dienstleister betrieben werden.
- den Bereitstellungs- und Betriebskosten der ausschließlich von EKUS genutzten zentralen IT-Ressourcen, einschließlich der hierbei benötigten personellen Ressourcen.[5]
- den Kosten für die Durchführung aller nach den Vorgaben des EKUS-Nutzergremiums bzw. des zentralen Dienstleisters notwendigen funktionalen und betrieblichen EKUS-Tests, einschließlich der Kosten für die Erstellung der benötigten Testunterlagen.
- den anteiligen Bereitstellungs- und Betriebskosten der von EKUS mitgenutzten querschnittlichen Services (z.B. Backup).

Die oben genannten Kostenblöcke umfassen auch den jeweiligen Mehrbedarf an internem Personal und externer Beratungs- und Unterstützungsleistung. Eine detaillierte Bezifferung der Kosten ist erst nach Abschluss des in Abstimmung befindlichen EKUS-Software-Pflege- und Weiterentwicklungsvertrags mit dem Fh-IVI sowie weiteren Abstimmungen mit dem Fh-IVI zur Notwendigkeit von SW-Anpassungen oder anderweitigen Customizing-Maßnahmen bei SE-Netz möglich.

§ 15. Auftragsdatenverarbeitung

Beim technischen Betrieb der für EKUS bereit gestellten IT-Infrastruktur und bei der Erbringung der Dienstleistungen darf der zentrale Dienstleister in Übereinstimmung mit seinen internen Sicherheitsbestimmungen externe Unterstützung in Anspruch nehmen. Die Auftragsdaten-verarbeitung wird durch die separate „Vereinbarung zur Auftragsdatenverarbeitung im Rahmen von EKUS“ geregelt.

§ 16. Datenschutz

Die Unterstützung mobiler Endgeräte beschränkt sich auf die Bereitstellung einer mobilen Anwendung (App). Die Lieferung sicherer mobiler Endgeräte sowie die Bereitstellung einer IT-Infrastruktur für den sicheren Betrieb mobiler Endgeräte sind nicht Gegenstand dieser Vereinbarung. Gleiches gilt für Beratungs- und Unterstützungsleistungen im Bereich mobiler Endgeräte.

§ 17. IT-Sicherheit

Gemäß Schutzbedarfsfeststellung wurde in allen drei Grundwerten Verfügbarkeit, Vertraulichkeit und Integrität der Schutzbedarf „hoch“ festgelegt.

[5] Bei über Virtualisierungstechnologien bereitgestellten Ressourcen der IT-Infrastruktur des zentralen Dienstleisters werden anteilige Bereitstellungs- und Betriebskosten umgelegt.

Verfügbarkeit:
Die maximal tolerierbare Ausfallzeit des Backend pro Einzelereignis liegt bei kleiner gleich 8 Stunden, aber größer als 2 Stunden. Die Jahresverfügbarkeit beträgt größer gleich 99%, aber kleiner als 99,8%.

Vertraulichkeit:
Durch Offenlegung von Informationen oder deren Kenntnisnahme durch Unbefugte wird die Aufgabenerfüllung erheblich beeinträchtigt. Die Offenlegung von Informationen oder deren Kenntnisnahme durch Unbefugte hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.

Integrität:
Durch fehlerhafte oder fehlende Informationen wird die Aufgabenerfüllung erheblich beeinträchtigt. Die Nutzung fehlerhafter oder unvollständiger personenbezogener Daten mit Auswirkung auf z. B. die informationelle Selbstbestimmung Einzelner hat erhebliche Folgen für die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.

Für die Schnittstellen zum Karten-Server wie auch zu den einzelnen Ortungsservern müssen die Verfügbarkeiten im Einzelnen festgelegt werden.

Es sind die Vorgaben gemäß BSI-Standard 100-2 [5] zu berücksichtigen. Darüber hinaus sind die Vorgaben gemäß BSI-Standard 100-3 [6] (Schutzbedarf „hoch“) zu berücksichtigen.

Die bestehenden im CNP-Verbund geltenden Regelungen zu Meldewegen und Changemanagement finden hier Berücksichtigung.

§ 18. Salvatorische Klausel

(1) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise ungültig sein oder werden, wird hiervon die Gültigkeit anderer Teile nicht berührt. Die Parteien verpflichten sich, die ungültigen Bestimmungen durch gültige Regelungen zu ersetzen, die dem rechtlichen und wirtschaftlichen Gehalt der ungültigen Bestimmung weitgehend entspricht.

(2) Eventuell offenbar werdende Lücken dieser Vereinbarung sind durch Regelungen zu schließen, die die Parteien bei Kenntnis der Lücken im Interesse beider Parteien nach Treu und Glauben getroffen hätten.

§ 19. Inkrafttreten, Einheitlichkeit und Kündigung

(1) Diese Vereinbarung tritt mit Unterzeichnung in Kraft.

(2) Eine einseitige Kündigung dieser Vereinbarung durch einzelne EKUS-Teilnehmer ist nicht zulässig.

(3) Hebt der AK II seinen Beschluss zum Betrieb eines bundesweiten EKUS auf oder verändert die Rahmenbedingungen wesentlich, endet diese Vereinbarung 9 Monate~~n~~ nach Verkündung des neuen AK II Beschlusses automatisch, soweit bis dahin nicht eine einvernehmliche Vertragsanpassung zustande gekommen ist.

(4) Die Möglichkeit einer außerordentlichen Kündigung, insbesondere wegen grober und anhaltender Verstöße gegen das Datenschutzrecht, bleibt unberührt. Von den Vertragsparteien ist sicherzustellen, dass laufende Maßnahmen durch eine Kündigung nicht gefährdet werden. Die Kündigung hat schriftlich zu erfolgen.

(5) Mit dem Wirksamwerden einer außerordentlichen Kündigung verliert der entsprechende EKUS-Teilnehmer alle Rechte aus dieser Vereinbarung, insbesondere wird sein Zugang zum EKUS-Zentralsystem gesperrt. Für alle übrigen Teilnehmer ändert sich zunächst nichts. Die Vereinbarung bleibt in Kraft und wird zu unveränderten Bedingungen fortgeführt. Den Finanzierungsanteil des ausgeschiedenen Mitglieds übernimmt der übergangsweise der Bund. Der zentrale Dienstleister hat jedoch das Recht, beim EKUS-Nutzergremium oder einer übergeordneten Instanz eine Veränderung des Kostenverteilungsschlüssels mit dem Ziel zu beantragen, die nicht mehr gedeckten Kosten gleichmäßig auf die verbleibenden EKUS-Teilnehmer aufzuteilen.

Anhang 1: Details zum Servicelevel des Rechenzentrumbetriebs

Auf Basis der IT-Infrastruktur und der Betriebsorganisation des zentralen Dienstleisters werden die für bundesweit bzw. international genutzte polizeilichen Anwendungen mit hohem Schutzbedarf erforderlichen Servicelevels bereits seit vielen Jahren erreicht.

Der zentrale Dienstleister sichert die Umsetzung aller in die eigene Zuständigkeit fallenden betrieblichen Maßnahmen auch für EKUS zu. Darüber hinaus hängt das Servicelevel von einer angemessenen Mitwirkung des Software-Anbieters ab, insbesondere in den Bereichen Software-Pflege und Support. Diese Mitwirkungsleistungen werden in noch zu schließenden Supportverträgen mit dem Fh-IVI vereinbart. Eine endgültige Zusage zum Servicelevel der Gesamtanwendung kann vor Abschluss des Beschaffungsverfahrens nicht gemacht werden.

Kommentar [HM2]: Löschen nach Abstimmung der Einzelabrufe mit dem Fh-IVI

Der Servicelevel bei den Endanwendern hängt zudem von Verfügbarkeit und Störanfälligkeit aller an der Bereitstellung und Aufrechterhaltung der Ende-zu-Ende-Verbindung beteiligten IT-Geräte und IT–Infrastrukturen (z.B. Mobilgerät, drahtloses und drahtgebundenes Kommunikationsnetz, MDM, zentrales Rechenzentrum (RZ)) ab. Zusagen kann der zentrale Dienstleister nur für seine eigenen Anteile machen.

Konkret garantiert der zentrale Dienstleister folgende Service-Leistungen:

- Zwei räumlich getrennte Rechenzentren mit zwei auf separaten Trassen verlaufenden Kommunikationsverbindungen.
- Redundante, räumlich getrennte Anbindungen ans CNP.
- Besonderer Zutrittsschutz zu den RZ-Räumlichkeiten.
- Redundante über beide RZ verteilte HW-Ausstattung.
- Redundante über beide RZ-verteilte Datenspeicherung.
- Automatisierte Betriebsüberwachung
- 7*24 h besetzter RZ-Leitstand mit Zugriffsmöglichkeit auf 7*24h Rufbereitschaft des Betriebspersonals und auf 7*24h Support der wesentlichen Infrastrukturlieferanten.
- 7*24h User Help Desk.
- Transaktionsgesicherte datenschutzrechtliche Protokollierung in einer Datenbank.
- Etablierte Verfahren zur Abstimmung bund-/länderübergreifender oder international relevanter Veränderungen an der IT-Infrastruktur (z.B. in den Bereichen INPOL und Schengen), u.a. definierte Wartungsfenster.
- Umfangreiche IT-Sicherheitsmaßnahmen nach Vorgaben des BSI und der internen Sicherheitsbeauftragten, mit regelmäßigen Sicherheitsaudits durch die Länder.

Kooperationsvereinbarung

zwischen

dem Freistaat Sachsen, vertreten durch das Landeskriminalamt, Neuländer Straße 60, 01129 Dresden (im Folgenden: LKA SN),

vertreten durch den Präsidenten, Herrn Petric Kleine,

und

der Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastraße 27, 80686 München,

vertreten durch Frau Kathrin Werner und Herrn Lars-Friedrich Krone

für Leistungen ihres
Fraunhofer-Instituts für Verkehrs- und Infrastruktursysteme (im Folgenden: Fraunhofer IVI)

Präambel

Grundlage für diese Kooperationsvereinbarung ist die Angebotsaufforderung vom 22. Januar 2015 (Az.: 32-0275.80/19/14) mit der dazugehörigen Auftragserteilung vom 19.Februar 2015 (Forschungs- und Entwicklungs- (FuE-)-Auftrag), aufgrund dessen das Fraunhofer IVI für das LKA SN ein mobiles Sprach- und Datenkommunikationsnetz/ Einsatzführungssystem für Spezialeinheiten und Spezialkräfte des LKA SN (SE-Netz) entwickelt, welches das LKA SN in die praktische Nutzung überführt und die hierfür erforderlichen taktischen Einsatz- und Führungsregeln schafft bzw. anpasst (im Folgenden: Basispaket)

Ziel ist ein partnerschaftliches Miteinander aller Kooperationspartner.

Das Ziel der ursprünglichen Kooperationsvereinbarung wird mit dieser Verlängerung auf folgende Zielstellungen erweitert:

- Weiterentwicklung von SE-Netz zu einer einheitlichen mobilen Einsatzkommunikations- und Unterstützungssoftware der Spezialeinheiten und Spezialkräfte der Polizeien des Bundes und der Länder (EKUS) sowie des Zolls im Rahmen eines FuE-Projekts
- Kooperative Bereitstellung einer zentralen, für alle behördenübergreifenden Einsätze nutzbaren (EKUS)-Instanz unter Federführung des BKA.
- Zusammenarbeit als Entwicklungs- bzw. Testpartner für die Weiterentwicklung, Erstellung von Testberichten, Erstellung technisch-organisatorischer Fachanforderungen.

Bereits während des bis 31.Dezember 2016 befristeten FuE-Projekts mit dem Az.: 32-0275.80/19/14 unterstützte und förderte das LKA SN im Rahmen seiner Möglichkeiten und gesetzlichen Aufgaben die Weiterentwicklung des Systems und gibt anderen Behörden bei Interesse die Möglichkeit, sich an dem FuE-Projekt zu beteiligen. Die bestehende Kooperationsvereinbarung vom 4./17. November 2016 soll hiermit angepasst und bis zum 31.12.2025 verlängert werden.

Die Kooperationsvereinbarung enthält Regelungen zur Zusammenarbeit, insbesondere zum gemeinsamen Wissens- und Erfahrungsaustausch und zu den Verwertungsrechten der Ergebnisse des FuE-Projekts.

§ 1 Gegenstand der Vereinbarung

Gegenstand dieser Vereinbarung ist

1. die Weiterentwicklung von SE-Netz zu einer mobilen Einsatzkommunikations- und Unterstützungssoftware (EKUS) der Spezialeinheiten und Spezialkräfte der Polizeien des Bundes und der Länder und des Zolls,
2. die Bestimmung und Erbringung von Unterstützungsleistungen für den Betrieb der Software,
3. die Einräumung dauerhafter, unwiderruflicher und unkündbarer nicht ausschließlicher Nutzungsrechte zu Gunsten der Kooperationspartner sowie weitergehender Rechte im Sicherungsfall.
4. die im Interesse der Gewährleistung von Sicherheit und Ordnung der Bundesrepublik Deutschland eingeschränkte Berechtigung von Fraunhofer IVI zur Verwertung und Weiterentwicklung der Software. Dies schließt die Zusammenarbeit mit Dritten und/oder die Vergabe von entgeltlichen Lizenzen von Fraunhofer IVI an Dritte mit ein, soweit dadurch der Hauptzweck der Kooperation, die Bereitstellung von EKUS für die Polizeien des Bundes und der Länder und den Zoll nicht gefährdet wird.

§ 2 Kommunikation, Kooperation

Die Kooperationspartner werden in Bezug auf den in der Präambel beschriebenen Vertragsgegenstand wechselseitig

- Informationen, Erfahrungen und Erkenntnisse zu den vereinbarten Themen und Inhalten austauschen und bewerten sowie

- sich über den Fortgang des Projektes, insbesondere dessen Teil-, und Endergebnisse, regelmäßig gegenseitig unterrichten.

Die jeweiligen Aufgaben und Zuständigkeiten sind in §5 genauer geregelt.

§3 Dauer, Kündigung, Evaluation, Beziehungen der Vertragspartner untereinander/ Federführung, Geschäftsstelle

3.1 Diese Kooperationsvereinbarung wird über den 31. Dezember 2020 hinaus verlängert und endet am 31. Dezember 2025. Im Zeitraum vom 01.01.2026 bis zum 31.12.2027 wird das Fraunhofer IVI weiterhin vollwertigen Support, insbesondere Pflegeleistungen für die EKUS Software inkl. Schließen und Beseitigung von Sicherheitslücken zur Verfügung stellen; Einzelheiten hierzu werden in einem separaten Vertrag festgelegt.

3.2 Eine außerordentliche Kündigung der Vereinbarung ist zulässig bei Vorliegen eines wichtigen Grundes. Vor Ausspruch einer solchen Kündigung ist zunächst das Verfahren nach § 7 einzuleiten, es sei denn, ein weiteres Abwarten mit der Kündigung ist für den

Kündigenden unzumutbar. Ein wichtiger Grund liegt insbesondere dann vor, wenn die für Fraunhofer IVI anfallenden Kosten für die Weiterentwicklung des EKUS Systems nicht getragen werden, obwohl sie angemessen sind und Fraunhofer IVI zuvor die Kooperationspartner vergeblich schriftlich aufgefordert hat für einen Kostenausgleich zu sorgen. Nach Zugang der außerordentlichen Kündigung wird diese nach Ablauf von sechs Monaten wirksam. Erklären sich einer oder mehrere der Kooperationspartner innerhalb der Frist des Satzes 4 schriftlich, in haushaltsrechtlich verbindlicher Form dazu bereit, die Kosten zu tragen oder für eine anderweitige Finanzierung zu sorgen, wird die außerordentliche Kündigung endgültig nicht wirksam.

3.3 Die einzurichtende Geschäftsstelle (s. Absatz 5.3) legt pro Quartal mindestens einen Erfahrungsbericht dem Fraunhofer IVI vor. In diesen Erfahrungsbericht sollen – sofern diese in geeigneter schriftlicher Form der Geschäftsstelle vorliegen - auch Erkenntnisse der Polizeien anderer Länder, des Bundes und des Zolles miteinfließen.

3.4 Die Weiterentwicklung von EKUS erfolgt durch das Fraunhofer IVI aus den zur Verfügung stehenden Geldern. Entwicklungen zur Sicherheit müssen den IT-Sicherheitsstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entsprechen. Die Kooperationspartner verpflichten sich, bekannt gewordene Sicherheitsschwachstellen dem Fraunhofer IVI über die Geschäftsstelle unverzüglich mitzuteilen. Die Sicherheit und Lauffähigkeit des vom Fraunhofer IVI entwickelten Systems haben Vorrang vor jeglicher Weiterentwicklung. Die Kooperationspartner übernehmen die Verantwortung für die ordnungsgemäße Implementierung aller in ihren Zuständigkeitsbereich fallenden ~~EKUS-spezifischen~~ Sicherheitsvorgaben ~~des Fraunhofer IVI~~. Das Fraunhofer IVI trägt die Verantwortung für die Umsetzung aller notwendigen Sicherheitsvorkehrungen innerhalb der Entwicklung der EKUS Softwarekomponenten und definiert Handlungsempfehlungen für einen sicheren Betrieb. Die Kooperationspartner sind für die Sicherheit der IT-Infrastruktur/IT-Umgebung, in der EKUS betrieben wird (Server, Endgeräte und darauf laufende Software), und für die Sicherheit des Betriebs von EKUS sowie aller für den EKUS-Betrieb notwendigen Komponenten in der eigenen IT-Architektur/IT-Umgebung selbst verantwortlich. ~~Bei Kooperationspartnern, die einen lokalen EKUS-Server betreiben, umfasst das die Vorgaben für die Absicherung dieses Servers (z.B. notwendige Portfreischaltungen) und der zugehörigen IT-Infrastruktur. Das Fraunhofer IVI trägt die Verantwortung für die Umsetzung aller notwendigen Sicherheitsvorkehrungen innerhalb der Entwicklung der EKUS Softwarekomponenten. Die Kooperationspartner sind dafür verantwortlich, dass die vom Fraunhofer IVI übergebene Software in einer sicheren IT-Infrastruktur/IT-Umgebung betrieben wird~~.

3.5 Die Federführung der FuE-Kooperation geht mit ihrer Verlängerung vom LKA SN auf das BKA über. Das BKA stimmt diesem Wechsel, unter Beibehaltung des Inhaltes dieser Vereinbarung im Übrigen ausdrücklich zu. Das LKA SN richtet eine Geschäftsstelle ein, die die operative Koordination zwischen dem Fraunhofer IVI, dem BKA und den weiteren Kooperationspartnern übernimmt.

§ 4 Verbreitung/Bereitstellung an Dritte/Support

4.1 Im Hinblick auf die Zielsetzung, eine einheitliche EKUS Softwarelösung für die Bundesrepublik Deutschland zu entwickeln und zu etablieren, stimmt das LKA SN der Beteiligung weiterer Sicherheitsbehörden des Bundes und der Länder an dem bestehenden FuE-Projekt EKUS zu (Weiterentwicklung von SE-Netz zu einer einheitlichen mobilen Einsatzkommunikations- und Unterstützungssoftware der Spezialeinheiten und Spezialkräfte der Polizeien des Bundes und der Länder sowie des Zolls im Rahmen eines FuE-Projektes einschließlich kooperativer Bereitstellung einer zentralen, für alle behördenübergreifenden Einsätze nutzbaren EKUS-Instanz unter Federführung des BKA). Die von den weiteren Sicherheitsbehörden bereitgestellten finanziellen Mittel für das EKUS FuE-Projekt sind zweckgebunden und werden ausschließlich für das bestehende EKUS FuE-Projekt und dessen darauf aufbauende, im Kreis der EKUS Kooperationspartner einvernehmlich beschlossene Weiterentwicklungs- und Folgeprojekte verwendet. Die Vertragsbedingungen werden zwischen dem Fraunhofer IVI und der jeweiligen Behörde, möglichst unter Beibehaltung der bisherigen Bedingungen, Aufnahmeregelungen und FuE-Qualitätsstandards, verhandelt.

4.2 Die Aufnahme weiterer EKUS Projekt-/Kooperationspartner gemäß Ziffer 4.1 erfolgt bis zum 30.06.2019 nach folgendem Preismodell:

- Basispaket – bestehend aus einem Nutzungsrecht der Software an stationären und mobilen Endgeräten für bis zu 300 Nutzer: 80.000 €/netto,
- Basispaket mit Erweiterungen für bis zu 300 zusätzliche Nutzer: 140.000 €/netto
- Basispaket mit Erweiterungen für bis zu 600 zusätzliche Nutzer: 180.000 €/netto
- Basispaket mit Erweiterungen für bis zu 900 zusätzliche Nutzer: 220.000 €/netto

Die Preise gelten zunächst bis 30. Juni 2019. Ab dem 1. Juli 2019 werden sie jährlich an die gültigen Personalkostensätze und anhand der Systementwicklungsanforderungen des Fraunhofer IVI angepasst. Bis zum Abschluss einer entsprechenden Änderungsvereinbarung gelten die jeweils aktuellen Preise weiter. Neue EKUS Kooperationspartner erhalten die jeweils aktuelle Version der bundeseinheitlichen EKUS-Software.

Sofern die EKUS Einnahmen nicht ausreichen, um die vom EKUS Nutzergremium beschlossenen Anpassungen und Weiterentwicklungen vorzunehmen, werden die EKUS Parteien eine Regelung zur Finanzierung dieser Maßnahmen treffen, damit die EKUS Kooperation im nötigen Umfang aufrechterhalten wird. Das Fraunhofer IVI wird, sobald sich eine Finanzierungslücke abzeichnet, die Kooperationspartner umgehend informieren und den zu erwartenden Finanzbedarf darlegen.

Anpassungen und Weiterentwicklungen, die außerhalb der Aufgaben der Kooperation

nur mit einzelnen Kooperationspartnern realisiert werden sollen, sind zwischen dem Kooperationspartner und dem Fraunhofer IVI gesondert zu verhandeln und vom Bedarfsträger zu finanzieren. Solche Anpassungen und Weiterentwicklungen unterliegen dem Vetorecht des BKA, sofern diese unverhältnismäßigen Aufwände für das BKA verursachen oder mit unverhältnismäßigen betrieblichen Risiken oder Risiken für die Stabilität der Software bzw. des Gesamtsystems verbunden sind.

Die Nutzungsrechte werden als nicht ausschließliche und nicht unterlizenzierbare, jedoch dauerhafte, unwiderrufliche, unkündbare und übertragbare Rechte nach der Metrik „named user“ vergeben, d.h. für jede Person, die zur Nutzung von EKUS berechtigt ist, wird eine eigene Lizenz benötigt. Diese Lizenz deckt alle Zugriffswege (mobil und stationär) sowie den Zugang zu beliebig vielen verschiedenen EKUS-Instanzen (Bundes- und Landesbestände an Echt- und Testdaten) mit beliebig vielen Endgeräten ab. Die Lizenz berechtigt ebenfalls dazu, sämtliche weitere serverseitigen Komponenten, die zur Nutzung der EKUS Software erforderlich bzw. vorgesehen sind, insb. auch die Kommandooberfläche und den Kartenserver zu nutzen, wobei diese Komponenten auch von Personen genutzt werden dürfen, für die keine „named user“-Lizenz erworben wurde.

Die Lizenzen beinhalten o.g. Rechte auch für alle während der Laufzeit der Kooperation verfügbar werdenden neuen Programmstände (z.B. Updates, Upgrades, neuen Versionen) der EKUS Software und der weiteren Komponenten, die zur Nutzung der EKUS-Software erforderlich bzw. vorgesehen sind. Eine gesonderte Vergütung für die Nutzung der neuen Programmstände ist nicht zu zahlen; diese ist vielmehr mit dem Erwerb der ursprünglichen Lizenzen abgegolten.

Lizenzen, die bei Inkrafttreten dieser Vereinbarung bei den Mitgliedern der Forschungskooperation vorhanden sind, werden im Verhältnis 1:1 kostenfrei in „named-user“-Lizenzen umgewandelt.

4.3 Die erforderliche technische Unterstützung bei der Implementierung und dem Betrieb der Softwarelösung sowie die Fehler- und Störungsbeseitigung sowohl der zentralen als auch der mobilen Teile der EKUS Software (Support) erfolgt durch das Fraunhofer IVI und wird bis zum 30. Juni 2019 ohne weitere Vergütung gewährleistet.

Für den Zeitraum ab 01.07.2019 stellt das Fraunhofer IVI priorisierten Softwaresupport sowohl für alle zentral beim BKA betriebenen Instanzen als für die zum Zugriff auf diese Instanzen genutzten mobilen Teile der EKUS-Software bereit. Dieser priorisierte Softwaresupport wird durch das Fraunhofer IVI außerhalb der Forschungskooperation erbracht und ist daher in einem separaten Vertrag zwischen dem BKA als zentralem Dienstleister und dem Fraunhofer IVI zu regeln. Der Leistungsumfang entspricht dem des Supports gemäß Absatz 4.3, wird jedoch vorrangig vor Leistungen für andere Kooperations- bzw. Vertragspartner von Fraunhofer IVI erbracht. Das Fraunhofer IVI sagt

für diesen Support eine garantierte Ansprech- und Bearbeitungszeit an 5 Werktagen/Woche für jeweils 8 Stunden zu den üblichen Büro- und Geschäftszeiten zu, wobei entsprechende Anfragen des BKA (als Dienstleister) mit Priorität gegenüber allen anderen beim Fraunhofer IVI vorliegenden Anfragen des gleichen Schweregrads zu EKUS bearbeitet werden. Der priorisierte Softwaresupport deckt auch alle in den zentralen EKUS-Instanzen bereitgestellten Länderdatenbestände ab, jedoch keine Datenbestände/Instanzen, die von EKUS-Teilnehmern in eigener Zuständigkeit betrieben werden.

In diesem Vertrag ist auch die Hinterlegung der Quellcodes der EKUS-Software beim BKA und der Zugriff und die Nutzung desselben darauf im Sicherungsfall zu regeln.

Der Softwaresupport für lokale Instanzen, d.h. Instanzen, die von Kooperationspartnern in eigener Zuständigkeit betrieben werden, ist vom jeweiligen Bedarfsträger direkt beim Fraunhofer IVI zu beauftragen und selbst zu finanzieren. Der Softwaresupport für bereits im Betrieb befindliche lokale Instanzen von Kooperationspartnern, die bereits vor der Verlängerung der Kooperationsvereinbarung über den 31. Dezember 2020 hinaus beigetreten sind, wird gemäß der ursprünglichen Kooperationsvereinbarung bis zur Wirkbetriebsaufnahme von EKUS auf den Endgeräten des jeweiligen Kooperationspartners, längstens jedoch bis zum 31. Dezember 2020, fortgesetzt.

4.4 Das Fraunhofer IVI ist zur eigenen Verwertung und Weiterentwicklung von EKUS auf eigene Kosten berechtigt, soweit dadurch der Hauptzweck der Kooperation, die Bereitstellung von EKUS für die Spezialeinheiten und Spezialkräfte der Polizeien des Bundes und der Länder sowie des Zolls sowie deren Interessen, insbesondere die Gewährleistung der öffentlichen Sicherheit und Ordnung, nicht gefährdet werden. Die erforderlichen Verträge schließt das Fraunhofer IVI. Soweit es sich um Behörden und Organisationen mit Sicherheitsaufgaben (BOS) oder Ordnungsaufgaben aus der EU handelt, bedarf es keiner Genehmigung. Soweit Fraunhofer IVI beabsichtigt, Verträge mit anderen Dritten zu schließen, ist mindestens zwei Monate zuvor das BKA schriftlich über den avisierten Vertragspartner und den geplanten Liefer- und Leistungsumfang zu informieren. Soweit das BKA die o.g. Interessen gefährdet sieht, kann es binnen eines Monats seit Zugang der Information sein Veto einlegen. Fraunhofer IVI hat das Recht, den geplanten Vertrag, insbesondere dessen Leistungsumfang so anzupassen, dass die Bedenken des BKA ausgeräumt werden. Gelingt dies nicht, d.h. hält das BKA sein Veto aufrecht, ist Fraunhofer IVI nicht berechtigt, den Vertrag mit dem anderen Dritten zu schließen. Eine Gefährdung der Interessen kann auch darin liegen, dass die Identität des Vertragspartners bzw. des Endkunden und/oder der Leistungsumfang unklar sind.

§5 Abgrenzung der Zuständigkeiten

5.1 Gemäß AK II-Beschluss entscheidet ein EKUS-Nutzergremium über polizeifachliche und technische Fragen der EKUS-Weiterentwicklung. Diesem EKUS-Nutzergremium,

dessen Mandatierung zum 27.07.2018 von allen EKUS-Teilnehmern akzeptiert wurde, gehören alle EKUS-Nutzer als stimmberechtigte Mitglieder an, soweit es sich dabei um Polizeibehörden des Bundes und der Bundesländer handelt.

Das Fraunhofer IVI ist ständiges Gastmitglied im EKUS-Nutzergremium. Als Gast kann das Fraunhofer IVI von der Behandlung einzelner besonders sensibler Tagesordnungspunkte ausgeschlossen werden. Über den Ausschluss des Fraunhofer IVI entscheidet das EKUS-Nutzergremium im Einzelfall. Im Übrigen umfasst die Gastmitgliedschaft mit Ausnahme des Stimmrechts alle Rechte eines ordentlichen Mitglieds, insbesondere ein Vortrags- und Antragsrecht.

Die Einnahmen aus dem Lizenzverkauf an die Mitglieder der Forschungskooperation, die das Fraunhofer IVI während der Laufzeit dieses Vertrags mit der EKUS-Software erzielt, kann es unter Beachtung der Zweckbindung (§4.1) und unter Einbeziehung der Anwender eigenständig für gezielte Forschungs- und Entwicklungsarbeiten zur Innovation und Zukunftssicherung der Software einsetzen. Geplante Aktivitäten größeren Umfangs sind dem Nutzergremium vorab zu berichten.

Das BKA als zentraler Dienstleister kann die Umsetzung von Entscheidungen des Gremiums ablehnen, sofern diese unverhältnismäßige Aufwände für das BKA verursachen oder mit erheblichen oder mit unverhältnismäßigen betrieblichen Risiken verbunden sind.

5.2. In Ausnahmefällen können dringliche Entscheidungen, die im Wege einer Befassung des EKUS Nutzergremiums nicht zeitgerecht herbeigeführt werden können, unter Beachtung von Absatz 5.4 in polizeifachlichen Fragen von der EKUS-Geschäftsstelle, in entwicklungstechnische Fragen vom Fraunhofer IVI und in betriebstechnischen Fragen vom BKA als zentralem Dienstleister getroffen werden, soweit die Entscheidungen technisch mit vertretbarem Aufwand umsetzbar sind und nicht mit betrieblichen Risiken einhergehen. Die EKUS Geschäftsstelle, Fraunhofer IVI und BKA werden sich – soweit dies zeitlich möglich ist - wechselseitig vorab über entsprechende Entscheidungen informieren. Weiterhin werden sie das EKUS-Nutzergremium im Nachgang informieren.

5.3 Beim LKA SN in Dresden wird eine EKUS-Geschäftsstelle eingerichtet und der Projektgruppe „SE-Netz“ zugeordnet, die folgende Aufgaben wahrnimmt:

- Generell die Weiterentwicklung des Systems zu fördern.
- Sammlung und Vorprüfung neuer polizeifachlicher Anforderungen
- Koordination der softwareseitigen Umsetzung der vom EKUS-Nutzergremium verabschiedeten priorisierten Aufgabenliste
- Ansprechstelle für Softwarepflege- und Supportanforderungen, die sich auf EKUS-Instanzen beziehen, die von EKUS Teilnehmern in eigener Zuständigkeit betrieben werden.

- Weitere Aufgaben, die sich aus der Weiterentwicklung des Systems ergeben können.

5.4 Die EKUS-Geschäftsstelle beim LKA SN, das Fraunhofer-IVI und das BKA stimmen sich fortlaufend hinsichtlich der jeweils vorliegenden EKUS-Anforderungen und des jeweiligen Entscheidungsbedarfs über polizeifachliche und technische Fragen ab, um eventuelle Wechselwirkungen, Widersprüche und Konflikte frühzeitig zu erkennen.

5.5 Supportanfragen, die sich auf die zentral im BKA betriebene EKUS-Instanzen beziehen, müssen ab Verfügbarkeit des priorisierten Supports direkt an den Helpdesk des BKA gestellt werden.

§ 6 Haftung

Jeder der Kooperationspartner haftet für Schäden, die in seinem Verantwortungsbereich ihre Ursachen haben. Das Fraunhofer IVI steht für die Anwendung wissenschaftlicher Sorgfalt sowie die Einhaltung der allgemein anerkannten Regeln der Technik ein, nicht aber für das tatsächliche Erreichen des FuE-Ziels. Die Haftung der Kooperationspartner ist auf Vorsatz und grobe Fahrlässigkeit beschränkt.

§ 7 Konflikte, Mediation

Bei Meinungsverschiedenheiten über die Durchführung oder Auslegung der Kooperationsvereinbarung sowie über das Bestehen eines außerordentlichen Kündigungsgrundes verpflichten sich die Kooperationspartner zur Aufnahme von Verhandlungen innerhalb einer Frist von einem Monat mit dem Ziel, eine einvernehmliche Lösung herbeizuführen.

§ 8 Datengeheimnis

Die Kooperationspartner kommen überein, die jeweiligen Mitarbeiterinnen und Mitarbeiter, die mit dem Gegenstand dieser Vereinbarung in Kontakt kommen, auf das Datengeheimnis zu verpflichten.

Soweit ein Zugang zu Echtdaten durch Fraunhofer IVI nicht auszuschließen ist oder in sonstigen Fällen, in denen eine Auftragsverarbeitung vorliegt, ist zwischen Fraunhofer IVI und dem BKA eine Vereinbarung zur Auftragsverarbeitung gemäß EU-DSGVO sowie gemäß Teil 3 BDSG 2018 und dem jeweils für den Kooperationspartner anwendbaren Landesdatenschutzgesetz zu schließen.
Eine solche Vereinbarung deckt nur Instanzen ab, die in den Rechenzentren des BKA betrieben werden. Für Instanzen, die die Kooperationspartnern in eigener Zuständigkeit betreiben, sind zwischen den Beteiligten separate Vereinbarungen zu schließen.

Weiterhin sind Sicherheitsüberprüfungen nach Sicherheitsüberprüfungsgesetz erforderlich, und zwar eine Ü2-Sabotageschutz für Mitarbeiter, die Zugang zu Echtdaten oder zu einem Rechenzentrum des BKA erhalten, und eine Ü1 für alle anderen Mitarbeiter, die an der Softwareentwicklung EKUS beteiligt sind oder Informationen über die IT-Infrastruktur oder die Betriebsabläufe innerhalb der IT des BKA erhalten.

§ 9 Schlussbestimmungen

9.1 Änderungen und Ergänzungen zu dieser Vereinbarung müssen als solche gekennzeichnet sein und bedürfen zu ihrer Rechtswirksamkeit der Schriftform.

9.2 Die Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., das BKA und das LKA SN werden Veröffentlichungen nur im gegenseitigen Einvernehmen und unter Nennung nur solcher Kooperationspartner, die eine solche Nennung auch wünschen, durchführen. Dabei werden Urheberrechte von Fraunhofer IVI und die Geheimhaltungsaspekte berücksichtigt.

9.3. Die Vereinbarung tritt mit ihrer Unterzeichnung in Kraft.

9.4. Sollte eine Bestimmung dieses Vertrages unwirksam, nichtig, etc. sein, so berührt dies die Wirksamkeit der Vereinbarung als Ganzes nicht. Die unwirksame, nichtige, etc. Bestimmung soll vielmehr durch eine Regelung ersetzt werden, die rechtlich zulässig ist und die inhaltlich und wirtschaftlich dem am Nächsten kommt was die Kooperationspartner mit der unwirksamen, nichtigen, etc. Bestimmung gemeint haben. Das gilt auch im Fall einer Vertragslücke.

Dresden, den

Landeskriminalamt Sachsen

……

Petric Kleine

München, den

Fraunhofer-Gesellschaft zur Förderung
der angewandten Forschung e.V.

……

Kathrin Werner

……

Lars-Friedrich Krone

Wiesbaden, den

Bundeskriminalamt

_____