Deutscher Bundestag **Drucksache 21/6634**

21. Wahlperiode 23.06.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Jan Köstering, Donata Vogtschmidt, Violetta Bock, weiterer Abgeordneter und der Fraktion Die Linke
– Drucksache 21/6364 –

Umsetzungsstand des Programms P20 im Juni 2026

Vorbemerkung der Fragesteller

Anknüpfend an frühere Kleine Anfragen (zuletzt Bundestagsdrucksache 20/13130 will die fragenstellende Fraktion mit dieser Kleinen Anfrage den aktuellen Sachstand des Programms P20 zur Modernisierung und Vereinheitlichung der Datenhaltung und Datenverarbeitung bei der deutschen Polizei erfragen. Das Vorhaben erhält zusätzliche Brisanz aufgrund der von der Bundesregierung beschlossenen Gesetzentwürfe zur Einführung digitaler Ermittlungsbefugnisse im Rahmen der Gefahrenabwehr durch das Bundeskriminalamt (BKA) und die Bundespolizei (BPol) und der Strafprozessordnung. Nach dem Verständnis der Fragesteller können alle in den polizeilichen Datenverarbeitungssystemen gespeicherten Daten durch die geplante automatisierte Datenverarbeitung genutzt werden. Für das Testen und Trainieren von IT-Anwendungen bestehen hier nicht einmal die ansonsten geltenden Beschränkungen durch die verfassungsgerichtlichen Anforderungen an eine zweckändernde Nutzung von durch eingriffsintensive Maßnahmen erhobenen personenbezogenen Daten. Ausgeschlossen wird im Gesetzentwurf zwar die Verwendung von Informationen, die aus einer Wohnraumüberwachung oder dem Ausforschen von Smartphones und Computern stammen. Stammen die Informationen hingegen aus einer Telekommunikationsüberwachung oder von verdeckten Ermittlern bzw. Vertrauenspersonen der Polizei („V-Leute“), können sie verwendet werden (§ 22 Absatz 3 des Bundeskriminalamtgesetzes [BKAG] nach dem Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit, www.bundesregierung.de/breg-de/bundesregierung/bundeskanzleramt/kabinett-digitale-ermittlungsbefugnisse-2304936).

Vorbemerkung der Bundesregierung

Das in der Vorbemerkung der Fragesteller geäußerte Verständnis der Gesetzentwürfe zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit, zur Abwehr von Gefahren des internationalen Terrorismus sowie zur Änderung Strafprozessordnung – digitale Ermittlungsmaßnahmen, die am 29. April 2026 von der Bundesregierung beschlossen wurden, bedarf aus Sicht der Bundesregierung einer Präzisierung.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 23. Juni 2026 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Die Fragesteller äußern das Verständnis, dass alle in den polizeilichen Datenverarbeitungssystemen gespeicherten Daten durch die geplante automatisierte Datenverarbeitung genutzt werden könnten. Hierzu weist die Bunderegierung auf Folgendes hin:

Die Befugnisse zur automatisierten Datenanalyse unterliegen nach den o. a. Gesetzentwürfen hohen Tatbestandsvoraussetzung, sie dürfen ausschließlich bei einem Tatverdacht bezüglich einer Straftat nach § 100a Absatz 2 der Strafprozessordnung (StPO) oder einer konkretisierten Gefahr für besonders gewichtige Rechtsgüter angeordnet werden. Sie erlauben dafür den Zugriff auf die Daten, auf die die Polizeibehörde zur Erfüllung ihrer Aufgabe zugreifen darf (exemplarisch § 9b Absatz 1 Satz 1 BKAG-E). Dies umfasst exemplarisch für das Bundeskriminalamt insbesondere das Informationssystem nach § 13 BKAG sowie den polizeilichen Informationsverbund nach § 29 BKAG. Umfasst sind demnach nur Daten, die die Behörden rechtmäßig gespeichert und auf die sie bereits nach bisherigem Recht Zugriff haben. Ein Zugriff auf die Datenbestände anderer Behörden, die nicht Bestandteil des polizeilichen Informationsverbundes sind, ist nicht Gegenstand dieser Befugnisse. Dies gilt auch für Befugnisse zum Testen und Trainieren von IT-Produkten (exemplarisch § 22 Absatz 3 BKAG-E).

Des Weiteren äußern die Fragesteller das Verständnis, dass Befugnisse zum Testen und Trainieren von IT-Produkten die verfassungsgerichtlichen Anforderungen an die zweckändernde Verwendung personenbezogener Daten nicht beachteten. Hierzu weist die Bunderegierung auf Folgendes hin: Diese Befugnisse dienen dem Testen von IT-Produkten sowie Trainieren von KI-Systemen. Beide Tatbestandsvarianten zielen auf die Verbesserung der Funktionen selbst, sie ziehen keine polizeilichen Maßnahmen bezüglich der betroffenen Personen nach sich und sehen keine darüber hinausgehende Verarbeitung der Daten vor.

1. Wie ist der aktuelle Sachstand beim Aufbau des Polizeilichen Informations- und Analyseverbundes (PIAV), insbesondere hinsichtlich

   a) der Umsetzung der Stufen 5 bis 7, wurde die Wirkbetriebsaufnahme Anfang März 2026 erreicht (vgl. Bundestagsdrucksache 20/13130, S. 6), und wenn nein, warum nicht?

Die Wirkbetriebsaufnahme der PIAV-Stufen 5 bis 7 erfolgte entsprechend der Meilensteinplanung fristgerecht zum 2. März 2026.

   b) Über welche Schnittstellen zu welchen Anwendungen und Datenbanken verfügen PIAV-Operativ und PIAV-Strategisch derzeit, und welche weiteren Schnittstellen sind derzeit vorgesehen oder bereits in Planung bzw. Implementierung (bitte für beide Systeme getrennt angeben)?

Der PIAV-Operativ besitzt neben den Schnittstellen zu den Zuliefer- und Abfragesystemen nur noch Schnittstellen zum Europol Informationssystem (EIS) und zum Abgleichservice (ABS). Weitere Schnittstellen sind nicht geplant. Der PIAV-Strategisch besitzt keine Schnittstellen zu anderen als den Zulieferungssystemen.

2. Wie ist der Stand des Aufbaus des Informationssystems des BKA nach § 13 BKAG?

   a) Wie ist die Zielarchitektur des Informationssystems des BKA?

Die Fragen 2 und 2a werden gemeinsam beantwortet.

Die Zielarchitektur des Informationssystems des BKA ist Bestandteil der Zielarchitektur des Datenhausökosystems des Programms P20. Innerhalb dieser Zielarchitektur sollen in Zukunft die Daten zur Vorgangs- und Fallbearbeitung, die Fahndungen nach Personen und Sachen sowie die Basis für statistische Auswertungen enthalten sein.

b) Welche Bestandssysteme und welche neuen Systeme sollen im Informationssystem zusammengeschlossen werden?

Die Zielarchitektur P20 reduziert die fragmentierte Datenhaltung in einzelnen Systemen. Die Daten werden verschiedenen Services auf Basis konkreter Berechtigungsregeln zur Ansicht zur Verfügung gestellt. Innerhalb des BKA werden in den Bestandssystemen hierzu Schritte zur Vorbereitung der Integration unternommen und die Planungen des Programms P20 unterstützt. Systeme, die auf eigenen gesetzlichen Grundlagen oder gesonderten Zwecken bestehen sind hiervon nicht betroffen.

c) Für welche Bestandssysteme und ggf. neuen Systeme wurde im Verlauf des iterativen und dynamischen Aufbauprozesses entschieden, sie nicht in das Informationssystem zu integrieren?

Die Arbeiten an der Planung dauern an.

d) Gibt es nach derzeitigem Stand einen projektierten Zeitpunkt zum Abschluss des Informationssystems, und welche Meilensteine sind bis dahin noch zu erreichen?

Die Transformation des Informationssystems insgesamt unterliegt zahlreichen Abhängigkeiten, die im Veränderungsprozess mitberücksichtigt werden müssen. Ein Abschluss ist derzeit noch nicht abschließend zu benennen, eine überwiegende Transformation in die Zielarchitektur wird für 2030 angestrebt.

e) Was sind die von der Bundesregierung benannten „Abhängigkeiten“, die in ihrer „Vielzahl“ im Veränderungsprozess berücksichtigt werden müssen (vgl. Bundestagsdrucksache 20/13130, S. 6)?

Hier sind mehrere Faktoren zu berücksichtigen. Zum einen sind Daten aus Informationssystemen mit verschiedenen nationalen und internationalen Partnern entsprechend der gesetzlichen Zuständigkeiten auszutauschen. Dies führt zu Anpassungen bis hin zum Neuaufbau von Schnittstellenfunktionalitäten. Des Weiteren wird die Abschichtung der Funktionen der heutigen Bestandsysteme iterativ erfolgen. Hierbei sind nicht alle Serviceangebote zu einem Stichtag durch alle Polizeien zu nutzen, was den Prozessen in der föderalen IT-Struktur entgegenkommen soll. Insgesamt bedingen die Einflussfaktoren eine weit über gewöhnliche Abschichtungs- und Transformationsprozesse hinausgehende Koordination und Abstimmung.

3. In welcher Art von technischem und organisatorischem Prozess soll

a) im Informationssystem des BKA (§ 13 BKAG) und

Im BKA-Vorgangsbearbeitungssystem ist die Kennzeichnung vollständig umgesetzt. Jedes Fachobjekt ist dort entsprechend dem im Programm P20 festgelegten XPolizei-Standard gekennzeichnet. Die Umsetzung der hypothetischen Datenneuerhebung orientiert sich an den im Rahmen des Programms P20 festgelegten Standards. Des Weiteren wird auf die Antwort zu Frage 3b verwiesen.

b) im Polizeilichen Informationsverbund (§ 29 BKAG)

zukünftig im Rahmen des Konzepts der „hypothetischen Datenneuerhebung“ kenntlich gemacht werden, welche Daten in welcher Eingriffsintensität erhoben wurden?

Die Umsetzung der hypothetischen Datenneuerhebung erfolgt im polizeilichen Informationsverbund bzw. im Datenhausökosystem mittels des sogenannten Ticket-Label-Abgleichs. Anhand von farblichen Labels (grün, gelb, orange, rot), wird die grundrechtliche Eingriffsschwere der spezifischen Maßnahme symbolisiert. Für eine Abfrage wird ein Ticket erstellt, bei dem zwischen zwei Abfragegründen unterschieden wird (repressive Abfrage und präventive Abfrage). Die Funktionsweise des Ticket-Label-Abgleichs wurde mit der Bundesbeauftragen für den Datenschutz und die Informationsfreiheit abgestimmt.

4. Welche technischen und organisatorischen Maßnahmen sind i. S. v. § 48 des Bundesdatenschutzgesetzes (BDSG) vorgesehen, um

a) im Informationssystem des BKA und

b) im polizeilichen Informationsverbund

bei der Verarbeitung besonderer Kategorien personenbezogener Daten einen geeigneten Schutz der Rechtsgüter der betroffenen Personen zu gewährleisten?

Es sind verschiedenste technische und organisatorische Maßnahmen vorgesehen, um sicherzustellen, dass die Verarbeitung besonderer Kategorien personenbezogener Daten sowohl im Informationssystem des BKA als auch im polizeilichen Informationsverbund unter Beachtung des besonderen Schutzbedürfnisses dieser Daten erfolgt. Dies umfasst unter anderem Maßnahmen zur Verwehrung des Zugangs zu den Verarbeitungsanlagen, Maßnahmen zur Gewährleistung, dass die zur Benutzung der Verarbeitungssysteme Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben, sowie Maßnahmen zur Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte. Außerdem werden Verarbeitungen protokolliert, um deren Überprüfbarkeit zu gewährleisten. Weitere Maßnahmen sind beispielsweise Schulungen der an der Datenverarbeitung Beteiligten zur Sensibilisierung und die Festlegung von Aussonderungsprüffristen.

5. Wie sind die Zahl und der Stand der Umsetzung der P20-Projekte, und in welchen Release Trains und Shared Services sind sie derzeit gebündelt?

8. Welche Projekte innerhalb der Release Trains und Shared Services konnten bislang erfolgreich abgeschlossen werden, und welche der entstandenen Produkte sind aktuell im Wirkbetrieb?

Die Fragen 5 und 8 werden gemeinsam beantwortet.

Das Programm P20 besteht aktuell aus 13 Release Trains (RTs) und 38 Projekten, die sich unter die einzelnen RTs gliedern.

Der RT Datenhausökosystem (DHÖS) ist nach der im Jahr 2025 angepassten Release Train Struktur in sechs untergeordnete RTs gegliedert:

I. RT DHÖS Basis 1

- Datenhaus – Entwicklung/im Wirkbetrieb
- Kernkomponenten – Entwicklung/im Wirkbetrieb

II. RT DHÖS Basis 2
- Identity Access Management (IAM) – aktiv
- Kataloge – aktiv
- Protokollierung – aktiv
- Geo – aktiv
- Querschnittsservices – aktiv
- Querschnittsservice Spracherkennung – aktiv
- Minimum Viable Product (MVP) KI-Plattform – aktiv

III. RT DHÖS Fachanwendungen 1 – Auskunft
- DHÖS Services – aktiv
- DHÖS Services Kern – aktiv
- Portierungen – aktiv
- P20-Strafanzeige und Verkehrsunfallaufnahme – aktiv

IV. RT DHÖS Fachanwendungen 2– Verbund
- INPOL-L Transformation – aktiv
- INPOL-Z Transformation – aktiv
- PIAV Transformation – aktiv
- INPOL Neuausrichtung – aktiv
- Fahndung – aktiv
- Deconfliction – aktiv
- P20-Lageanwendung – aktiv

V. RT DHÖS Fachanwendungen 3 – Auswertung und Analyse
- Komplexrecherche – aktiv
- Datenanalyseplattform – in Planung

VI. RT DHÖS Fachanwendungen 4 – Vorgang
- Vorgangsservices – in Planung

Der RT eFBS und PIAV umfasst fünf Projekte:
- eFBS – aktiv
- PIAV – Operativ – aktiv, in Wirkbetrieb
- PIAV-S PMK – aktiv
- PIAV-AQUA – aktiv
- DaFKa – aktiv

Der RT Justiz führt die beiden Projekte:
- Elektronische Akte in Strafsachen (EAS) – aktiv, in Wirkbetrieb
- Übermittlungslösung – aktiv

Daneben gibt es jeweils einen RT für die drei sogenannten interims-Vorgangsbearbeitungssysteme (iVBS) @rtus, PLX und IGVP, welche das jeweils gleichnamige Projekt führen. Der RT Zentrales Informations-Management Portal (ZIMP) führt das gleichnamige Projekt. Der RT Kommunikation und Einsatz führt aktuell das Projekt Messenger.

Darüber hinaus existieren weitere neun Projekte, welche keinen RTs zugeordnet sind, weil diese abgeschlossen wurden und sich im Wirkbetrieb befinden:

1. Extrapol Multimediaplattform – abgeschlossen, in Wirkbetrieb
2. Enterprise Architecture Management (EAM) – aktiv, in Wirkbetrieb
3. Wiederholungsprognose Assistent (WiPrAs) – abgeschlossen, in Wirkbetrieb
4. Kriminaltechnischer Informationsverbund Urkunden (KIVU) – abgeschlossen
5. Social Media Content Management Tool (SMCMT) – abgeschlossen
6. Onlinewache – abgeschlossen, in Wirkbetrieb
7. Einsatzprotokollsystem (EPS-FE) – abgeschlossen, in Wirkbetrieb
8. Polizeilicher Informationsaustausch bei Sporteinsätzen (PIAS 2.0) – abgeschlossen, in Wirkbetrieb
9. INSITU (Tatortdokumentation) – abgeschlossen, Weiterentwicklung als Fachlicher Service unter DHÖS Fachanwendungen 1

Im Programm P20 gibt es neben den RTs und den einzelnen Projekten auch die sogenannten 12 Shared Services, die programmübergreifende Unterstützungsleistungen für die einzelnen RTs anbieten und demnach auch keinen RTs zugeordnet sind. Dabei handelt es sich um nachfolgend gelistete Shared Services:

1. Koordinierungsstelle Programmmanagementoffice
2. Competence Center Fachlichkeit
3. Competence Center Architektur
4. Produktmanagement
5. UI/UX (User Interface/User Experience und Barrierefreiheit)
6. Presse- und Öffentlichkeitsarbeit und Veränderungsmanagement
7. Recht und Datenschutz
8. Zentrales Anforderungsmanagement
9. Ressourcenmanagement
10. Change Request-Koordination
11. Testfactory
12. Risikobewertung und Sicherheitskonzepte

6. Bei welchen der P20-Projekte kommt Künstliche Intelligenz (KI) i. S. d. Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-VO) zum Einsatz, und welche davon werden als Hochrisiko-Systeme i. S. v. Annex III der KI-VO gewertet (bitte bei der Auflistung auch aufführen, für welches der Systeme eine Folgenabschätzung vorliegt)?

Derzeit kommt bei den P20-Projekten keine künstliche Intelligenz i. S. der Verordnung 2024/1689 zum Einsatz.

7. Welche der Services und Anwendungen, die im Rahmen von P20 entwickelt werden, sollen Polizeibeamtinnen und Polizeibeamten auf mobilen Endgeräten zur Verfügung gestellt werden, und wird dabei auf Cloud-basierte Lösungen zurückgegriffen (wenn ja, welche Mindestanforderungen bestehen dabei jeweils hinsichtlich des Standortes des Rechenzentrums, der Personen mit Zugang zu Software und Daten, nichteuropäischer Anteile im Vorstand involvierter Software-Anbieter oder Software-Dienstleister, Open Source beim verwendeten Cloud-Stack und Anwendungssoftware sowie Einhaltung der Kriterienkataloge C5 und C3A des Bundesamts für Sicherheit in der Informationstechnik [BSI])?

Alle das Datenhausökosystem betreffende P20 Anwendungen werden nach aktuellen technischen Standards entwickelt und basieren auf modernen Cloud-Technologien. Hierdurch besteht grundsätzlich die Möglichkeit, alle diese Anwendungen sowohl über mobile als auch stationäre Endgeräte zu nutzen.

Der Betrieb der Services und Anwendungen erfolgt derzeit auf der BKA eigenen On-Premise Cloud (BKA-Cloud). Sofern perspektivisch weitere Cloud-Dienstleister eingebunden werden, müssen diese die vom BSI vorgegebenen Sicherheitsstandards erfüllen und eine Freigabe zur Verarbeitung von „VS-Nur für den Dienstgebrauch“ eingestuften Informationen vorweisen.

9. Wie sind der derzeitige Umsetzungs- und Planungsstand beim „Einzug“ der Landespolizeibehörden in das gemeinsame „Datenhaus“ der deutschen Polizei?

Zum gegenwärtigen Zeitpunkt sind die zwei Teilnehmerländer Rheinland-Pfalz sowie Saarland produktiv an das Datenhaus angebunden. Im Rahmen des sogenannten Verfahrens zur beschleunigten Befüllung des Datenhauses, welchen vom obersten Gremium des Programms, dem Verwaltungsrats des Polizei-IT-Fonds, beschlossen wurde, ist vorgesehen, das Datenhaus bis Mitte 2027 mit den Daten aller Teilnehmer zu befüllen.

10. Welche Vorgangsbearbeitungssysteme werden derzeit vor der Einführung des einheitlichen Vorgangsbearbeitungssystems (eVBS) von den Bundes- und Landespolizeibehörden genutzt, und

Derzeit wird bei den Teilnehmern eine Vielzahl von Vorgangsbearbeitungssystemen (VBS) genutzt. Dies umfasst die bestehenden VBS der Länder sowie die drei sogenannten interims Vorgangsbearbeitungssysteme (iVBS).

a) wodurch unterscheiden sich die derzeit genutzten Vorgangsbearbeitungssysteme,

Diese Bestandssysteme unterscheiden sich sowohl in ihrer technischen Architektur als auch im fachlichen Funktionsumfang.

b) wie sind der derzeitige Stand und die Planung bei der flächendeckenden Umstellung auf das eVBS?

Eine Umstellung auf ein eVBS ist nicht geplant. Die Umstellung auf die drei iVBSe (PLX, IGVP, @rtus) schreitet voran. Die ersten Teilnehmer haben bereits von ihrem VBS auf ein iVBS gewechselt.

11. Sind neben den Vorgangsbearbeitungssystemen des BKA und der Landespolizeien auch Verbunddateien und weitere Dateien und Datenbanken (Falldateien etc.) in das SB-Datenhaus (SB = Sachbearbeitung) integriert, und wenn ja, welche der Verbunddateien?

Derzeit sind keine Vorgangsbearbeitungssysteme oder Fallbearbeitungssysteme in das Datenhaus integriert. Lediglich die Vorgangs- und Falldaten werden per Schnittstellen an das Datenhaus ausgeleitet. Verbunddateien werden im Rahmen einer Transformation betrachtet und werden in den nächsten Jahren iterativ abgeschichtet.

12. Wie wurden die Verbunddateien „technisch modernisiert“ (Bundestagsdrucksache 20/13130, S. 9), und wann werden die Verbunddateien vollständig durch ein neues System der Verbunddatenhaltung abgelöst sein?

Die konkrete Umsetzung der Modernisierung der Verbunddaten hat Mitte 2026 begonnen. Hierzu zählen sowohl Daten und Funktionen des PIAV und des INPOL. Für die Datenbereitstellung des PIAV ist geplant, dass im zweiten Halbjahr 2027 im Datenhausökosystem P20 eine Überführung der PIAV-OZ-Daten erfolgen kann, um im nächsten Schritt die Dateien des PIAV-Operativ abzulösen. Für das System INPOL sollen erste Services aus dem Aufgabenfeld der Fahndung und des Erkennungsdienstes ebenfalls in der zweiten Jahreshälfte 2027 zur Verfügung stehen. Die Transformation insgesamt wird hierbei aber eine über 2027 hinausgehende Zeitspanne andauern. Die Zeitplanung orientiert sich hierbei an den übergeordneten Zeitzielen des Transformationspfades des Programms P20.

13. Welche Fachanwendungen der Teilnehmer an P20 sind derzeit an das föderale Identity- and AccessM-Managementsystem (f-IAM) angeschlossen, und bei welchen Fachanwendungen steht die Integration noch aus?

Die Frage in Bezug auf die Fachanwendungen der Teilnehmer kann von der Bundesregierung nicht beantwortet werden, da die Anbindung von Systemen der Landespolizeien nicht in ihre Verantwortung fällt. Alle P20 Fachanwendungen werden an das IAM angeschlossen, hier handelt es sich um einen dynamischen Prozess, die der allgemeinen Transformationsplanung unterliegt.

14. Wie weit ist die Umsetzung einer Eigenentwicklung für die verfahrensübergreifende Recherche und Analyse, die als Alternative zu kommerziellen Produkten dienen soll, im BKA oder Bundesministerium des Innern (BMI) mittlerweile gediehen, und

Innerhalb des Programms P20 wird derzeit unter enger Einbeziehung der Teilnehmer der Aufbau von Fähigkeiten der Auswertung und Analyse im Datenhausökosystem vorangetrieben. Ziel ist es, in den nächsten Jahren erste Funktionalitäten bereitzustellen. Eine finale Entscheidung hinsichtlich der hierfür zu nutzenden Technologie(n) wurde noch nicht getroffen; angestrebt wird weiterhin eine souveräne Lösung im Einklang mit dem bestehenden Rechtsrahmen.

a) wurden Festlegungen getroffen oder sind in der Entwicklung, auf welche Quellsysteme eine solche Anwendung zugreifen können sollte,

c) wurde mittlerweile definiert, welches der Kreis der zu verarbeitenden personenbezogenen Daten sein soll,

Sowohl die Definition von anzuschließenden Datenquellen als auch die geplante Nutzung personenbezogener Daten sind Gegenstand dieser derzeitigen Arbeiten. Neben dem fachlichen Nutzen, sind hier auch der rechtliche Rahmen im Allgemeinen und der Datenschutz im Besonderen fest definierte Leitplanken.

b) inwiefern und inwieweit soll bei der Analyse und Aufbereitung von Informationen in einem solchen System auf KI-Komponenten zurückgegriffen werden,

Eine abschließende Aussage kann hierzu zum aktuellen Zeitpunkt nicht getroffen werden, da dies u. a. von der finalen Ausgestaltung der Anwendung abhängig ist.

d) inwieweit ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in die Entwicklung einbezogen, und inwieweit wurden deren Empfehlungen dabei berücksichtigt?

Die Bundesbeauftrage für den Datenschutz und die Informationsfreiheit wird über die etablierten Informationskanäle und Austauschformate mit dem Programm P20 zum Fortschritt im Bereich Auswertung und Analyse informiert. Sobald weitergehende Schritte in Richtung Umsetzung in den o. g. Bereichen unternommen werden, werden für den spezifischen Themenbereich der Auswertung und Analyse gemeinsam passende Formate entwickelt, um die Bundesbeauftragte regelmäßig und umfassend einzubinden.

15. Welche Anbieter wurden durch Marktsichtungen, Ausschreibungen, Interessenbekundungen, Initiativangebote und Präsentationen („Pitches“) identifiziert, die Systeme zur automatisierten Auswertung anbieten und diese an die rechtlichen und praktischen Vorgaben aus dem BMI oder seinen Geschäftsbereichsbehörden anpassen könnten?

Im Programm P20 wurde zu Beginn dieses Jahres der Aufbau von Fähigkeiten zur Auswertung und Analyse im Rahmen eines modularen und hybriden Ansatzes beschlossen. Die benötigten Fähigkeiten sollen nunmehr über eine Kombination einzelner Module bereitgestellt werden, die neben Bestandsprodukten und Eigenentwicklungen auch marktverfügbare Kaufprodukte umfassen kann. Die weitere Ausgestaltung befindet sich im fachlichen Prüfprozess.

16. Sollen Lagefalldateien weiterhin in INPOL-Fall (INPOL = Informationssystem der Polizei) außerhalb von PIAV-Operativ und dem Datenhaus-Ökosystem (DHÖS) weitergeführt werden, und wie ist die weitere Planung innerhalb des Programms P20 für die Lagefalldateien?

Bis zur Bereitstellung der Abbildung der fachlichen Anforderungen innerhalb des Datenhausökosystems werden INPOL-Fall-Dateien erforderlich sein. PIAV-Operativ konnte zwar eine Mehrzahl der Funktionen der INPOL-Fall-Funktionen ablösen, aber für die Überhänge bedarf es übergangsweise mancher INPOL-Fall-Anwendungen.

17. Wurde mittlerweile entschieden, wie mit den Tatmittelmeldediensten weiter verfahren werden soll (vgl. Bundestagsdrucksache 20/13130, S. 11)?

Die Tatmittelmeldedienste sind derzeit noch nicht Teil der Transformationsbetrachtungen in das Datenhausökosystem.

18. Sind die Datenmigrationskonzepte für die bisherigen Verbunddateien des BKA in das neue Verbundsystem nach § 29 BKAG mittlerweile weiter spezifiziert worden, wie ist die Meilensteinplanung für die Migration dieser Daten, und welche sind die Eckpunkte der Transformationsplanung mit den jeweiligen Verbundteilnehmern?

Für den PIAV-Operativ bestehen derzeit entsprechende Planungen. Die Voraussetzungen um die verbundrelevanten Daten, die heute an den PIAV-Operativ geliefert werden, im Datenhaus abzubilden, werden bis Mitte 2027 im Datenhausökosystem geschaffen. Eine Visualisierung der PIAV-Verbunddaten über P20-Produkte wird parallel realisiert werden. In diesem Zusammenhang wird die hyDaNe- und BKAG-konforme Abbildung der Verbunddaten im Datenhaus umgesetzt. Es entsteht somit die Basis, um die bisherigen PIAV-Operativ-Zentral-Dateien im weiteren Verlauf abzulösen.

Für das INPOL-System werden Fahndungs- und Erkennungsdienstliche Daten im Datenhausökosystem erfasst, bearbeitet und gelöscht werden können. Parallel zur angestrebten Servicebereitstellung im zweiten Halbjahr 2027 erfolgen weitere Datenerschließungen des INPOL-Systems und auch der Aufbau der Schnittstellenfunktionen zu externen nationalen und internationalen Partnern.

19. Wie sieht derzeit die Bilanz der verausgabten Haushaltsmittel für die Umsetzung des Programms P20 sowohl innerhalb der Haushaltsmittel für das BKA als auch bei den vom BMI für den Polizei-IT-Fonds aus (IT = Informationstechnik; bitte Soll-Ist-Vergleich nach Haushaltsjahren angeben)?

Zur Beantwortung der Frage 19 wird auf die beigefügte Anlage verwiesen.*

20. Von welchen Ansätzen geht die Bundesregierung bei der Planung für die weitere Umsetzung des Programms P20 in den genannten Haushaltstiteln bzw. Titelgruppen aus?

Zur Beantwortung der Frage 20 wird ebenfalls auf die beigefügte Anlage verwiesen.*

21. In welcher Weise plant die Bundesregierung bei der Umsetzung der Gesetzentwürfe für die Einführung digitaler Ermittlungsbefugnisse in der Gefahrenabwehr und Strafverfolgung (Beschlüsse des Bundeskabinetts vom 29. April 2026) den automatisierten Abgleich biometrischer Daten hinsichtlich

Die Gesetzentwürfe zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit, zur Abwehr von Gefahren des internationalen Terrorismus sowie zur Änderung Strafprozessordnung – digitale Ermittlungsmaßnahmen, die am 29. April 2026 von der Bundesregierung beschlossen wurden, sehen Befugnisse

* Von einer Drucklegung der Anlage wird abgesehen. Diese ist auf Bundestagsdrucksache 21/6634 auf der Internetseite des Deutschen Bundestages abrufbar.

zum automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet (biometrischer Internetabgleich) vor. Die Vorschriften im Bundeskriminalamtgesetz, Bundespolizeigesetz und in der Strafprozessordnung erlauben es, bereits vorliegende biometrische Daten – z. B. ein Lichtbild – zur Abwehr von Gefahren sowie zur Verhütung und Verfolgung von Straftaten von auch im Einzelfall erheblicher Bedeutung mit im Internet öffentlich zugänglichen Bildern biometrisch abzugleichen. Zudem ist eine entsprechende Befugnis im Asylgesetz vorgesehen.

Als Ziele der Maßnahmen zur Strafverfolgung und Gefahrenabwehr sind die Identifizierung, Aufenthaltsermittlung, Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen mit anderen Straftaten oder Gefahren vorgesehen. Die Befugnisse sind subsidiär zu anderen Maßnahmen. Adressaten der Regelung können im Bereich der Strafverfolgung Tatverdächtige und Beschuldigte, im Bereich der Gefahrenabwehr polizeipflichtige Personen sein. Für andere Personen besteht eine Begrenzung der Maßnahme auf die Zwecke der Identifizierung und Aufenthaltsermittlung sowie eine gesonderte Güterabwägung (exemplarisch § 9a Absatz 2 Nummer 2 BKAG-E).

Die im Rahmen der Befugnisse erhobenen personenbezogenen Daten sind nach Durchführung des biometrischen Internetabgleichs unverzüglich zu löschen (exemplarisch § 9a Absatz 4 Satz 1 BKAG-E). Eine dauerhafte Speicherung ist nicht erlaubt. Ein Abgleich mit Echtzeitdaten ist unzulässig (exemplarisch § 9a Absatz 1 Satz 2 BKAG-E). Es bestehen besondere Pflichten zur Datensicherheit und zur Protokollierung (exemplarisch § 9a Absatz 4 Satz 2 bis 4 BKAG-E).

Die Vorschriften im Bundeskriminalamtgesetz und Bundespolizeigesetz sehen ein abgestuftes Konzept vor, nach dem die Durchführung des biometrischen Internetabgleichs grundsätzlich durch die Polizeibehörde selbst erfolgen muss. Sofern dies technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist, darf die Durchführung durch eine öffentliche oder nichtöffentliche Stelle eines Mitgliedstaats der Europäischen Union erfolgen (exemplarisch § 9a Absatz 5 BKAG-E). Sofern auch dies technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist, kann die Durchführung durch eine öffentliche oder nichtöffentliche Stelle in einem Drittstaat erfolgen. Dies ist nur zum Zwecke des Schutzes der nationalen Sicherheit und aufgrund einer richterlichen Anordnung erfolgen (exemplarisch § 9a Absatz 8 BKAG-E). Im Bereich der Strafprozessordnung ist vorgesehen, dass der biometrische Internetabgleich nur durch die Strafverfolgungs- bzw. Polizeibehörde selbst erfolgen darf.

a) der Nutzung und Weiterentwicklung des Gesichtserkennungssystems (GES) des BKA,

Das bereit seit 2008 bestehende Gesichtserkennungssystem des Bundeskriminalamtes dient dem Abgleich biometrischer Daten mit dem polizeilichen Datenbestand. Die o. g. Befugnisse erlauben den Abgleich biometrischer Daten mit öffentlich zugänglichen Daten und sind insoweit nicht einschlägig.

b) der Anschaffung weiterer Systeme zum Abgleich biometrischer Daten aus den öffentlich zugänglichen Teilen des Internets (ggf. bitte auch ausführen, welche der derzeit bekannten Drittanbieter solcher Systeme in Betracht gezogen bzw. nicht in Betracht gezogen werden sollen),

Eine Entscheidung über einzelne Anbieter oder Produkte ist wesentlich von den rechtlichen Rahmenbedingungen abhängig, die sich derzeit im Gesetzgebungsverfahren befinden.

c) des Aufbaus eigener Referenzdatenbanken mit aus den öffentlich zugänglichen Teilen des Internets erhobenen biometrischen Gesichtsbildern und anderen biometrischen Daten,

Eine dauerhafte Speicherung von Daten auf Grundlage der o. g. Befugnisse ist ausgeschlossen.

d) des Aufbaus von Datenbanken zur Speicherung von Bildern aus Videoüberwachung oder Bildaufnahmen aus körpernah getragenen Aufzeichnungsgeräten (zum Beispiel „Bodycams“ oder Erfassungs-Apps wie MobileFortify), und welche Datenbanken stehen hierfür derzeit bei BKA, Bundespolizei und Zoll zur Verfügung?

Personenbezogene Daten, die im Rahmen der polizeilichen Aufgabenwahrnehmung erhoben wurden, fallen nicht unter die Tatbestandsvoraussetzung der öffentlich zugänglichen Daten aus dem Internet. Die Weiterverarbeitung dieser Daten richtet sich nach den entsprechenden gesetzlichen Regelungen.

22. Inwieweit sollen die in Frage 18 genannten Systeme und Datenbanken auch für die sogenannte Fernidentifizierung genutzt werden?

Die Bundesregierung versteht den in der Frage verwendeten Begriff der Fernidentifizierung als biometrische Fernidentifizierung im Sinne von Artikel 3 Nummer 41 der Verordnung (EU) 2024/1689. Der durch den Bezug auf Frage 18 thematisierte polizeiliche Informationsverbund nach § 29 BKAG dient dem Zweck der Zurverfügungstellung polizeilicher Daten. Die Vorschriften zum biometrischen Internetabgleich sehen vor, dass Daten, auf die die Polizeibehörde zur Erfüllung ihrer Aufgaben zugreifen darf, als Grundlage des Abgleichs verwendet werden dürfen (exemplarisch § 9a Absatz 1 Satz 1 BKAG-E). Dies umfasst auch Daten, die im polizeilichen Informationsverbunde nach § 29 BKAG gespeichert und dort den rechtlichen Vorgaben gemäß abgerufen werden können.

23. Wurden nach Kenntnis der Bundesregierung innerhalb des Programms P20 Anwendungen entwickelt oder geplant oder bereits in den Testlauf gebracht, die einen biometrischen Gesichtsabgleich unmittelbar vor Ort, etwa im Rahmen einer Personenkontrolle, mit einem digitalen Endgerät durch Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte ermöglichen?

Im Rahmen des Programms P20 wurden bislang keine Anwendungen im Sinne der Frage entwickelt oder getestet. Die aus der EU-Interoperabilitätsagenda resultierenden verpflichtenden Anforderungen zur biometrischen Abfrage der auf Ebene der EU bereitgestellten Interoperabilitätsadapter werden perspektivisch im Rahmen der P20-Anwendung „P20-Suche“ abgebildet.

24. Sind der Bundesregierung Systeme bekannt, die biometrische Referenzdatenbanken aufbauen oder bereits aufgebaut haben, die nicht unter die Regelungen der KI-Verordnung und damit nicht unter das Verbot des KI-gestützten Aufbaus einer solchen biometrischen Datenbank gemäß Artikel 5 Absatz 1e der KI-Verordnung fallen, und welche sind das?

Die Frage richtet sich nach dem Verständnis der Bundesregierung darauf, ob es Produkte gibt, die eine rechtlich zulässige Umsetzung der Befugnisse zum biometrischen Internetabgleich ermöglichen. Zum Anwendungsbereich des Ver-

bots nach Artikel 5 Absatz 1 Buchstabe e der Verordnung (EU) 2024/1689 weist die Bundesregierung darauf hin, dass diese in Bezug auf die nationalen Sicherheit nach Artikel 2 Absatz 3 der Verordnung (EU) 2024/1689 keine Anwendung findet Den Anforderungen an die nationale Sicherheit unterfallen nach der Rechtsprechung des Europäischen Gerichtshof insbesondere terroristische Aktivitäten (Europäischer Gerichtshof, Urteil vom 6. Oktober 2020, Rechtssachen C-511/18, C-512/19 und C-520/18, Randnummer 135. Zudem gilt das o. g. Verbot nicht, sofern für das Auslesen der Daten keine KI-Systeme eingesetzt werden (vgl. Leitlinien der Europäischen Kommission zur Auslegung von Artikel 5 der Verordnung über künstliche Intelligenz, Randnummer 234). Zur Prüfung und Entscheidung über einzelne Anbieter oder Produkte wird auf die Antwort zu Frage 21b verwiesen.

25. Teilt die Bundesregierung die Befürchtung der Fragensteller, dass durch die Möglichkeit eines biometrischen Abgleichs durch eine nichtöffentliche Stelle außerhalb der EU (§ 9a Absatz 5 BKAG-E in der Kabinettfassung) als Auftragsdatenverarbeiterin des BKA Unternehmen solche Abgleiche vornehmen, die weder der Datenschutz-Grundverordnung noch der KI-Verordnung der EU unterfallen und damit rechtswidrig personenbezogene Daten verarbeiten, und wie soll eine rechtswidrige Datenverarbeitung wirksam ausgeschlossen werden?

Die Gesetzentwürfe der Bundesregierung für das Bundeskriminalamtgesetz und Bundespolizeigesetz erlauben zum Zwecke des Schutzes der nationalen Sicherheit und aufgrund einer richterlichen Anordnung die Durchführung des biometrischen Internetabgleichs durch eine öffentliche oder nichtöffentliche Stelle in einem Drittstaat, sofern andere Optionen technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich sind (exemplarisch § 9a Absatz 6 BKAG-E, zu den weiteren Tatbestandsvoraussetzungen vgl. Vorbemerkung zu Frage 21). Damit liegen taugliche Rechtsgrundlagen für die Polizeibehörden im Anwendungsbereich der nationalen Sicherheit vor. Insoweit finden EU-rechtliche Vorgaben nach Artikel 2 Absatz 3 der Verordnung (EU) 2024/1689 sowie der Richtlinie (EU) 2016/680 (Erwägungsgrund 14) keine Anwendung.

26. Teilt die Bundesregierung die Ansicht der Fragensteller, dass durch die Gestaltung der Befugnisnorm § 9a Absatz 1 Satz 1 BKAG-E („mit Daten, auf die es zur Erfüllung seiner Aufgaben zurückgreifen darf“) auch solche biometrischen Daten in einen automatisieren Abgleich einbezogen werden können, die nicht im öffentlich zugänglichen Internet, sondern im eingeschränkt zugänglichen Internet (Deep Web) abrufbar sind und die das BKA zu beliebigen anderen Zwecken gespeichert hat (und wenn nein, bitte begründen)?

Unter die Formulierung „Daten, die das Bundeskriminalamt zur Erfüllung seiner Aufgaben zugreifen darf“, fallen ausschließlich Daten, die das Bundeskriminalamt auf Grundlege der Weiterverarbeitungsvorschriften speichern darf. Dies ist nur der Fall, wenn die Weiterverarbeitung personenbezogener Daten für die Aufgabenerfüllung des Bundeskriminalamtes im Einzelfall erforderlich ist.

27. Plant die Bundesregierung derzeit die Schaffung von Rechtsgrundlagen für die biometrische Fernidentifizierung, und wenn ja,

    a) auf welche Datenquellen sollen entsprechende Systeme zugreifen dürfen und

b) zu welchen Zwecken soll eine solche biometrische Fernidentifizierung vorgenommen werden?

28. Soll den Zielen der Bundesregierung nach eine biometrische Fernidentifizierung auch in Fällen, die über Fragen der nationalen Sicherheit und des Militärs hinausgehen, zur Anwendung kommen können?

Die Fragen 27 und 28 werden gemeinsam beantwortet.

Die Bundesregierung versteht den in der Frage verwendeten Begriff der biometrischen Fernidentifizierung im Sinne von Artikel 3 Nummer 41 der Verordnung (EU) 2024/1689 als übergeordneten Begriff. Zur Schaffung von Befugnissen zum biometrischen Internetabgleich wird auf die Antwort zu Frage 21 verwiesen. Hinsichtlich der Schaffung von Befugnissen zur Nutzung von biometrischen Echtzeit-Fernidentifizierungssystemen im Sinne von Artikel 3 Nummer 42 der Verordnung (EU) 2024/1689 ist die Meinungsbildung innerhalb der Bundesregierung noch nicht abgeschlossen.

29. Inwiefern plant die Bundesregierung, durch die in Frage 24 genannten Rechtsgrundlagen oder auch durch bestehende Gesetze künftig Sportveranstaltungen und deren Gäste biometrisch zu überwachen, im Sinne eines fortlaufenden Abgleichs von Bildern aus der Videoüberwachung mit polizeilichen Datenbeständen?

a) Schließt die Bundesregierung aus, dass es dabei zu einer (ggf. auch retrograden) biometrischen Analyse großer Teile der Gäste von Sportveranstaltungen im Zuge von Sicherungs- und Ermittlungsmaßnahmen kommen könnte?

b) Schließt die Bundesregierung aus, dass dabei diskriminierende Algorithmen zum Einsatz kommen (und wenn ja, wie)?

c) Schließt die Bundesregierung aus, dass dabei auch eine Datenübermittlung an Dritte im nichteuropäischen Ausland oder an Server-Standorte im Ausland erfolgt (und wenn nein, warum nicht)?

Die Fragen 29 bis 29c werden gemeinsam beantwortet.

Das Anfertigen von Foto- und Videoaufzeichnungen im Rahmen von Sportgroßveranstaltungen obliegt in der Regel dem Veranstalter. Polizeirechtliche Maßnahmen zur Gefahrenabwehr – wie auch die Datenverarbeitung im Kontext des Einsatzes von Videotechnik – im Kontext von Sportgroßveranstaltungen erfolgen größtenteils auf der Grundlage landesrechtlicher Normen, für deren Vollzug und Überprüfung überwiegend die Polizeibehörden und Gerichte der Länder zuständig sind. Im Falle des Erfordernisses strafrechtlicher Ermittlungen gelten die Vorschriften der StPO.

30. Wird sich die Bundesregierung, ausgehend von der Antwort zu Frage 2 auf Bundestagsdrucksache 21/5451, auf der kommenden Konferenz der Innenminister und -senatoren (IMK) dafür einsetzen, dass alle Bestrebungen befürwortet werden, die Fußballveranstaltungen sicherer gestalten, und inwiefern ist eine vorherige Prüfung der Verhältnismäßigkeit, Angemessenheit, Geeignetheit und Erforderlichkeit dieser Bestrebungen und der damit verbundenen technischen Instrumente im Vorfeld der IMK geplant (wenn geplant, bitte den Prozess genauer ausführen)?

Es wird auf die Antwort zu Frage 29 verwiesen. Weiterhin wird auf die Antwort der Bundesregierung zu Frage 2 der Kleinen Anfrage der Fraktion Die Linke auf Bundestagsdrucksache 21/5451 verwiesen: „Die Federführung für die durch die IMK und der Sportministerkonferenz (SMK) eingesetzte

Bund-Länder-offenen-Arbeitsgruppe (BLoAG) „Fußball ohne Gewalt“ liegt beim Land Hamburg. Im Rahmen dieser Gremienarbeit bringt das BMI seine Fachexpertise ein. Das BMI befürwortet ausdrücklich alle Bestrebungen, Fußballveranstaltungen sicherer zu gestalten, und steht einer konstruktiven Weiterentwicklung der Instrumente offen gegenüber.“

Verhältnismäßigkeit, Angemessenheit, Geeignetheit und Erforderlichkeit sind Rechtmäßigkeitsvoraussetzungen bei der Durchführung von Maßnahmen, für die einen normierte Aufgabe und Befugnis vorliegen muss. Diese Prüfung wird von den zuständigen Behörden vor Vollzug der Maßnahme durchgeführt. Die Grundsätze, die für die Rechtmäßigkeit staatlichen Handelns gelten, wurden auch im Rahmen der Arbeit der BLoAG „Fußball ohne Gewalt“ angewandt.

31. Könnte sich nach Ansicht der Bundesregierung der Erkenntnisgewinn aus behördlichen Datensätzen durch Automatisierung und Datenzusammenführung mittels der im Rahmen von P 20 geplanten Veränderungen des Datenzugriffs, der Digitalisierung und Standardisierung erheblich verbessern, und wenn ja, aus welchen Gründen strebt die Bundesregierung dennoch ergänzend Befugnisse zur biometrischen Überwachung des öffentlichen Raums an?

Ziel des Programms P20 ist eine verbesserte Verfügbarkeit der bei der Polizei vorhandenen, rechtmäßig erhobenen Informationen und Daten. Die biometrische Fernidentifizierung demgegenüber verfolgt den Zweck, zur Abwehr von Gefahren sowie zur Verhütung und Verfolgung von Straftaten von auch im Einzelfall erheblicher Bedeutung eine Person, die dem im Gesetzesentwurf definierten Personenkreis zuzurechnen ist, zu identifizieren oder deren Aufenthaltsort zu ermitteln, den Sachverhalt zu erforschen oder Zusammenhängen mit anderen Straftaten oder Gefahren zu ermitteln.

Anlage zur Kleinen Anfrage des Abgeordneten Jan Köstering u. a. und der Fraktion Die Linke; BT-Drucksache 21/6364

Zu 19. Den nachstehenden Tabellen sind die SOLL-IST-Vergleiche für die zentral verantworteten Bundesmittel (ZSB, darunter fallen die Mittel des BKA) sowie für den Polizei-IT-Fonds (PIF), die für die Umsetzung des Programms P20 angesetzt und verausgabt wurden für die Haushaltsjahre 2020-2026/2027 zu entnehmen.

Übersicht zentral verantwortete Bundesmittel (Zentralstellenbudget, ZSB):

	2020*	**2021***	**2022***	**2023***	**2024***	**2025**	**2026**	**2027**
SOLL Ansatz Kap. 0624 (in T Euro)	68.858	18.561	61.182	61.182	61.182	102.182	111.178	113.830
Reste Vorjahr Kap. 0624	117.648	142.525	87.246	65.100	45.258	19.750	41.805	-
SOLL Ansatz Kap. 0612, 0611 (in T Euro)	1.648	1.092	691	1.000	1.000	1.000	1.000	1.000
SOLL Gesamt (in T Euro)	**188.154**	**162.178**	**149.119**	**127.282**	**107.440**	**122.932**	**153.983**	**114.830**
IST Gesamt (in T Euro)	**34.035**	**64.433**	**72.531**	**66.124**	**72.950**	**73.110**	**23.109**	**-**

* gerundet

Polizei-IT-Fonds (PIF) Gesamt (Zahlen anhand Jahresfinanzberichte / Wirtschaftspläne erstellt)

	2020	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**
SOLL (in T Euro)	25.165	45.663	68.909	72.950	75.248	92.864	116.843
PIF 1. Teil	25.165	45.663	68.220	72.950	74.115	71.405	76.500
PIF 2. Teil			689	0	1.133	21.459	40.343
IST (in T Euro)	7.285	19.139	39.514	85.556	93.382	89.703	-
PIF 1. Teil	7.285	19.139	39.514	85.556	92.802	77.321	-
PIF 2. Teil	0	0	0	0	580	12.382	-

Bundesmittel 0602 (BMI Haushalt)

	2020	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**
SOLL (in T Euro, gem. Bundeshaushalt)	4.383	7.953	12.811	13.065	12.553	21.620	23.424

PIF 1. Teil (in T Euro) (gem. WiPl)**		7.952	12.751	12.176	12.553	12.429	13.317
PIF 2. Teil (in T Euro) (gem. WiPl)	-	-	-	-	-	9.191	10.107
IST Gesamt (in T Euro)		19.139	39.514	85.556	90.343	-	-
Bundesmittel (in T Euro)	7.155	4.942	7.373	8.037	11.307	20.775	-
Länder (in T Euro)	20.783	14.197	32.141	48.285	53.649	66.712	-
PIF 1. Teil (BMI; in T Euro)	7.155	4.942	7.373	8,037	11.307	12.152	-
PIF 2. Teil (BMI; in T Euro)	-	-	-	-	-	8.623	-

** Wirtschaftsplan

Zu 20. Die geplanten Ansätze für die weitere Umsetzung des Programms P20 sind nachfolgender Tabelle zu entnehmen. Die Ansätze entsprechen denen der aktuellen Haushaltsaufstellungsverfahren und sich noch nicht beschlossen. Es wird zudem eine kapitelübergreifende Umschichtung in Höhe von zwei Mio. Euro aus dem ZSB für den PIF angestrebt.

	2027	**2028**	**2029**	**2030**
SOLL gemäß letzten beschlossenen Eckwerten (in T Euro) (BMI, PIF-Anteil)	25.105	24.972	24.512	24.512
Plan gem. aktuellen Haushaltsaufstellungsverfahren (BMI; PIF-Anteil; in T Euro)	27.105	26.972	26.512	26.512
SOLL-Ansatz Kap. 602 (ZSB; in T Euro)	78.500	-	-	-

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333