KÖNIGREICH BELGIEN
Föderaler Öffentlicher Dienst
Auswärtige Angelegenheiten, Außenhandel und Entwicklungszusammenarbeit

Polizei

ibz Föderaler Öffentlicher Dienst Inneres

Empfehlungen der Taskforce in Bezug auf neue Initiativen der Gemeinden zur Verbesserung der Dienstleistungen für die Bürger

Inhaltsverzeichnis

Einleitung **2**

1. Hintergrund **3**

2. Projektarten **3**

2.1 Selbstbedienungsterminal - Kioskterminal **3**

2.1.1 Am Schalter einzureichende Anträge 4

2.1.2 Identifizierung des Antragstellers 4

2.1.3 Soft- und Hardware des Kioskterminals 5

2.1.4 Verantwortlichkeiten der Gemeindeverwaltungen 5

2.2 Hauslieferung **6**

2.2.1 Vertragliche Haftung 6

2.2.2 Betreffende Dokumente 7

2.2.3 Schutz personenbezogener Daten 8

2.2.4 Rückverfolgbarkeit und Status der Reisepässe 9

2.2.5 Identifizierung des Empfängers 10

2.2.6 Separater Sealbag für Reisepässe, die nach Hause geliefert werden sollen? 11

2.3 Selbstbedienungsautomat **11**

2.3.1 Sicherheitsrisiken 12

2.3.2 Identifizierung des Antragstellers 12

2.3.3 Verfahrensrechtliche Verpflichtungen 12

2.4 Mobiles Büro **13**

3. Schlussfolgerungen **13**

Einleitung

Zuständige Behörden: FÖD Inneres, FÖD Auswärtige Angelegenheiten, Ausländeramt

Empfänger: die Gemeinden in Belgien

Betreffende Dokumente: gewöhnliche Reisepässe, Reisedokumente für Flüchtlinge, Staatenlose oder Ausländer, Personalausweise und Aufenthaltstitel

Berechtigte: Bürger, die in einer Gemeinde einen Antrag auf die vorerwähnten Dokumente stellen

Verordnungsgrundlage:

- Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- Verordnung (EU) 2025/1208 des Europäischen Parlaments und des Rates vom 12. Juni 2025 zur Erhöhung der Sicherheit der Personalausweise von Unionsbürgern und der Aufenthaltsdokumente, die Unionsbürgern und deren Familienangehörigen ausgestellt werden, die ihr Recht auf Freizügigkeit ausüben
- Gesetz vom 15. Dezember 1980 über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Ausweisen von Ausländern
- Gesetz vom 8. August 1983 zur Organisation eines Nationalregisters der natürlichen Personen, Artikel 8 (B.S. vom 21. April 1984)
- Gesetz vom 19. Juli 1991 über die Bevölkerungsregister, die Personalausweise, die Ausländerkarten und die Aufenthaltsdokumente (B.S. vom 3. September 1991)
- Gesetz vom 30. Juli 2018 über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten (B.S. vom 5. September 2018)
- Konsulargesetzbuch vom 21. Dezember 2013, Kapitel 10 "Pässe" (B.S. vom 21. Januar 2014)
- Gesetz vom 10. Februar 2015 über automatisierte Verarbeitungen personenbezogener Daten, die für belgische Pässe und Reisescheine erforderlich sind (B.S. vom 2. März 2015)
- Königlicher Erlass vom 8. Oktober 1981 über die Einreise ins Staatsgebiet, den Aufenthalt, die Niederlassung und das Ausweisen von Ausländern
- Königlicher Erlass vom 25. März 2003 über die Personalausweise (B.S. vom 28. März 2003)
- Rahmenmitteilung Integrale Sicherheit 2026-2029 - Teil IV Kapitel 9 Nr. 6

1. Hintergrund

In der Rahmenmitteilung Integrale Sicherheit 2026-2029 (Teil IV Kapitel 9 Nr. 6) wird erneut betont, dass die Bekämpfung von Identitätsbetrug für die Föderalbehörden weiterhin prioritär bleibt. Es wird gefordert, die Sicherheit der Ausstellungsverfahren weiter zu erhöhen, indem unter anderem die verordnungsrechtlichen Aspekte in Bezug auf Vorbeugung und Bekämpfung von Identitätsbetrug, die Sicherheitsaspekte in den Gemeinden usw. verstärkt werden.

Andererseits wenden sich seit einigen Jahren mehrere Gemeinden an den FÖD Inneres und den FÖD Auswärtige Angelegenheiten, um eine Stellungnahme zu Innovationsprojekten im Bereich Beantragung und Ausstellung von Identitäts-, Reise- und Aufenthaltsdokumenten zu erhalten: Self-enrolment-Kioskterminals, Hauslieferung, Dokumentenverteiler, mobile Büros (mobile kits) usw.

Diese Initiativen, die derzeit von den lokalen Behörden entwickelt werden, um den Dienst am Kunden zu verbessern, führen dazu, dass die Abläufe zur Ausstellung dieser Dokumente komplexer und manchmal auch betrugsanfälliger werden. Tatsächlich werden all diese Abläufe heute von zuständigen Beamten selbst geleitet.

Der Zweck der vorliegenden Unterlage besteht darin, den Gemeinden in Bezug auf diese Innovationsprojekte minimale Richtlinien und Anweisungen zu geben. Die Taskforce Identitätsbetrug möchte sicherstellen, dass solche Initiativen nicht gegen die Sicherheit der Abläufe zur Beantragung und Ausstellung von Dokumenten verstoßen, so wie sie in der Rahmenmitteilung Integrale Sicherheit 2026-2029 gefordert wird.

Da die betreffenden Gemeinden für die Durchführung dieser Projekte außerdem häufig Verträge mit privaten Firmen abschließen, die nicht vom FÖD Inneres und vom FÖD Auswärtige Angelegenheiten zugelassen sind, möchte die Taskforce die jeweiligen Verantwortlichkeiten der vorerwähnten FÖDs und der Gemeinden, die einen solchen Vertrag abschließen, genau festlegen.

Für eine bessere Lesbarkeit ist jede Richtlinie mit diesem Symbol leicht zu finden:

2. Projektarten

2.1 Selbstbedienungsterminal - Kioskterminal

Einige Gemeinden möchten in ihren Räumlichkeiten Selbstbedienungsterminals einrichten, an denen der Bürger seinen Antrag auf ein Dokument registrieren kann, ohne an einen Schalter gehen zu müssen.

2.1.1 Am Schalter einzureichende Anträge

Um Risiken zu begrenzen, dürfen nicht alle Anträge über ein Selbstbedienungsterminal eingereicht werden.

Folgende Anträge müssen immer am Schalter unter der Kontrolle eines zuständigen Beamten eingereicht werden:

- Erstanträge auf ein Dokument (automatisierte Kontrolle),
- Anträge infolge eines Verlusts, eines Diebstahls oder der Vernichtung eines Dokuments (automatisierte Kontrolle),
- Anträge, die in dringenden und äußerst dringenden Verfahren eingereicht werden,
- Anträge, die nicht am Kioskterminal abgeschlossen werden können: Problem der Gesichtserkennung, Unterschrift, Fingerabdrücke usw.,
- Anträge nichtbelgischer Staatsangehöriger, deren Aufenthaltstitel nur dann erneuert werden kann, wenn zusätzliche oder neue Nachweise wie die Arbeitsbescheinigung vorgelegt werden,
- Anträge auf Reisedokumente für Flüchtlinge, Staatenlose oder Ausländer,
- Anträge auf Diplomaten- oder Dienstpässe[1],
- Anträge der von Amts wegen gestrichenen Personen und der im Ausland ansässigen Personen (automatisierte Kontrolle),
- Anträge von Minderjährigen und von Personen, die unter dem Schutz gerichtlicher Maßnahmen stehen (automatisierte Kontrolle),
- Anträge von Personen, die von Polizei-, Gerichts- oder Sicherheitsbehörden ausgeschrieben wurden und sich entweder in Passban oder eIDban befinden (automatisierte Kontrolle).

2.1.2 Identifizierung des Antragstellers

Es ist unerlässlich, dass der Antragsteller, der seinen Antrag über das Kioskterminal einreicht, eindeutig identifiziert wird. Zu diesem Zweck führt er seinen Personalausweis in das Kioskterminal ein und gibt seinen PIN-Code ein.

Das System muss über ein Modul mit Gesichtserkennung[2] verfügen, um das vom Kioskterminal aufgenommene Foto mit Fotos von vorhergehenden Dokumenten zu vergleichen, oder über ein Modul für den Abgleich von Fingerabdrücken[3] verfügen, das von den betreffenden

[1] Die Gemeinden sind für die Registrierung von Anträgen auf Diplomaten- oder Dienstpässe nicht zuständig. Der FÖD Auswärtige Angelegenheiten kann sie jedoch ausnahmsweise ersuchen, als erweiterter Schalter zu handeln, um die biometrischen Daten der Antragsteller für diese Pässe zu registrieren. Diese Registrierung kann jedoch erst nach vorheriger Zustimmung des FÖD Auswärtige Angelegenheiten und am Schalter der Gemeinde erfolgen.
[2] Vergleich mit den Datenbanken der vorhergehenden Fotos (Pässe, eID und Aufenthaltstitel).
[3] "One-to-one"-Vergleich der Fingerabdrücke auf dem Chip des Dokuments.

FÖDs zugelassen ist. Die Verwendung eines solchen Moduls muss die rechtlichen Rahmenbedingungen erfüllen und eine bestimmte Ergebnisqualität gewährleisten. Aufgrund der geplanten Verarbeitungsvorgänge (Gesichtserkennung und/oder Abgleich von Fingerabdrücken) und der Tatsache, dass die Verarbeitung eine große Anzahl von Personen betreffen wird, ist eine Datenschutz-Folgenabschätzung erforderlich.

2.1.3 Soft- und Hardware des Kioskterminals

Die im Kioskterminal verwendete Software muss von den zuständigen Föderalbehörden anerkannt werden, um:

- die verschiedenen Abläufe zur Beantragung und Ausstellung der Dokumente zu vereinheitlichen,
- den Zugang zu den föderalen Datenbanken, die personenbezogene Erkennungsdaten enthalten, zu sichern,
- den Schutz personenbezogener Daten zu gewährleisten,
- externe Angriffe auf die Datenverarbeitungssysteme der Föderalbehörden zu vermeiden,
- die Verfügbarkeit und Durchführbarkeit der Datenverarbeitungssysteme zu gewährleisten,
- die Interoperabilität der in den verschiedenen Gemeinden eingerichteten Systeme zu gewährleisten,
- die Übereinstimmung des Systems und der Verfahren mit den europäischen eIDAS-Vorschriften zu gewährleisten, damit der belgische Staat seine Qualifizierung als "Trust Service Provider" nicht verliert.

Die Hardware des Kioskterminals muss von den zuständigen Föderalbehörden zugelassen werden, um:

- die Qualität und Sicherheit der verwendeten Systeme zu gewährleisten,
- die Interoperabilität der in den verschiedenen Gemeinden eingerichteten Systeme zu gewährleisten,
- externe Angriffe auf Datenverarbeitungssysteme der Föderalbehörden zu vermeiden,
- eine einheitliche Hardwarekonfiguration in allen Gemeinden zu gewährleisten.

2.1.4 Verantwortlichkeiten der Gemeindeverwaltungen

Die Nutzung von Selbstbedienungsterminals darf nur erfolgen, wenn in dem Raum, in dem die Kioskterminals installiert sind, ein für die Beantragung und Ausstellung von Identitäts-, Reise- und

Aufenthaltsdokumenten ermächtigter Gemeindebeamter physisch anwesend ist. Dieser muss eingreifen können, wenn Bürger auf Probleme bei der Registrierung ihres Antrags am Kioskterminal stoßen.

Die Aktivierung von Identitäts- und Aufenthaltsdokumenten muss immer am tatsächlichen Schalter erfolgen. Unter bestimmten Bedingungen kann die Ausstellung von Reisepässen ohne menschliches Eingreifen erfolgen (siehe Kapitel 2 Nr. 3 Selbstbedienungsautomat).

Die Gemeinde beschreibt die technischen und organisatorischen Maßnahmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betreffenden Personen zu gewährleisten, oder führt eine Datenschutz-Folgenabschätzung durch.

Die Gemeinde bestimmt einen technischen Verantwortlichen für die Kioskterminals, der beim FÖD Inneres angegeben werden muss. Der kommunale SPOC Identitätsbetrug wird bei vermutlichem Identitätsbetrug die Kontaktstelle für die zuständigen FÖDs sein.

2.2 Hauslieferung

Einige Gemeinden möchten den Bürgern über eine Privatgesellschaft Identitäts-, Reise- und Aufenthaltsdokumente nach Hause liefern. Andere Gemeinden gehen so bereits für Reisepässe vor.

Bevor solche Initiativen ins Leben gerufen wurden, zielte die Zentralisierung der Ausstellung von Identitäts-, Reise- und Aufenthaltsdokumenten darauf ab, das Risiko von Dokumentendiebstahl in den Gemeinden zu verringern. Es gilt zu verhindern, dass dieses Phänomen durch das Hinzufügen anderer, weniger sicherer Ausstellungsmethoden wieder auftritt.

Der zwischen der Gemeinde und der Privatgesellschaft geschlossene Vertrag muss daher die Integrität der Identitätskette gewährleisten, von der die Ausstellung des Dokuments nur das letzte Glied ist.

2.2.1 Vertragliche Haftung

Der FÖD Inneres und der FÖD Auswärtige Angelegenheiten stehen in keinem Rechts- oder Vertragsverhältnis zu der von der Gemeinde bestimmten Liefergesellschaft und können diese daher bei Problemen (Diebstahl, Verlust, Schaden, missbräuchliche Verwendung personenbezogener Daten, ...) nicht haftbar machen. Mit anderen Worten haften unsere FÖDs für Identitäts-, Reise- und Aufenthaltsdokumente nur bis zu dem Zeitpunkt, zu dem die Dokumente von der Produktionsgesellschaft an die Gemeinde geliefert werden. Bei einem Vertrag zwischen der Gemeinde und einem Auftragsverarbeiter muss auf Artikel 28 der Datenschutz-Grundverordnung (DSGVO) verwiesen werden.

Für die Strecke zwischen der Gemeinde und dem Bürger haftet allein die Gemeinde. Die Gemeinden müssen diese Haftung also selbst mit ihrem Kurierdienst regeln, denn zwischen ihnen besteht sehr wohl ein Rechts- und Vertragsverhältnis. Der FÖD Inneres und der FÖD Auswärtige Angelegenheiten raten den Gemeinden daher, in den Vertrag mit der Gesellschaft die notwendigen Bestimmungen in Bezug auf den Ausgleich aller Schäden aufzunehmen, die durch eine Hauslieferung entstehen können (Diebstahl, Verlust, Beschädigung, missbräuchliche Verwendung personenbezogener Daten, ...). Darüber hinaus müssen in diesem Vertrag die Bedingungen für die Ermächtigung des mit der Verarbeitung der Reisepässe beauftragten Personals festgelegt werden. Jede Form des Einsatzes von Subunternehmern durch die Privatgesellschaft, die von der Gemeinde unter Vertrag genommen wurde, ist verboten.

Aus diesen Gründen sollten dem betreffenden FÖD (Auswärtige Angelegenheiten; siehe Nr. 2.2.2 weiter unten) rechtzeitig bestimmte Informationen, wie der Name der unter Vertrag genommenen Gesellschaft, ihr Gesellschaftssitz, ihre Kontaktdaten und das Beginn- und Ablaufdatum des Vertrags mitgeteilt werden. Diese Informationen können der Direktion C2 Reise- und Identitätsdokumente des FÖD Auswärtige Angelegenheiten übermittelt werden: passeport@diplobel.fed.be.

2.2.2 Betreffende Dokumente

Die Ausstellung von **Identitäts- und Aufenthaltsdokumenten** bringt einen Abgleich der Fingerabdrücke des Inhabers sowie eine mögliche Aktivierung der Zertifikate auf diesen Dokumenten mit sich. Diese Handlungen dürfen keinesfalls von einer Privatgesellschaft ausgeführt werden. Sie müssen von einem befugten Gemeindebediensteten vorgenommen werden.

Darum ist eine Hauslieferung für diese Dokumente nicht möglich (außer in bestimmten Situationen über biometrische Stationen).

Bei **Reisepässen und Reisescheinen** hingegen ist ein Abgleich der Fingerabdrücke und eine Aktivierung der Zertifikate noch nicht anwendbar, sodass unter bestimmten, in den nachstehenden Kapiteln aufgeführten Bedingungen zwischen der Gemeinde und einer Privatgesellschaft ein Vertrag über die Hauslieferung geschlossen werden könnte.

Eine Hauslieferung ist jedoch nicht möglich:

- wenn der vorherige Reisepass bei der Beantragung des neuen Passes der Gemeinde nicht übergeben und durch sie annulliert wurde,
- wenn der FÖD Auswärtige Angelegenheiten Ihnen - auch nach Einreichung des Antrags - mitteilt, dass der Reisepass ohne seine vorherige Zustimmung nicht ausgestellt werden kann (Betrugsverdacht). In diesem Fall muss der Antragsteller bei der Gemeinde vorstellig werden.

2.2.3 Schutz personenbezogener Daten

Beim Abschluss eines Hauslieferungsvertrags muss die Gemeinde eine bestimmte Anzahl rechtlicher und praktischer Bedingungen in Bezug auf die Verarbeitung personenbezogener Daten erfüllen:

- **Sensible personenbezogene Daten auf dem Chip des Reisepasses:**

  Der Chip des Reisepasses enthält eine Reihe von personenbezogenen Daten des Inhabers:

  - personenbezogene Daten,
  - biometrische Merkmale (Foto, Fingerabdrücke).

  Im Gegensatz zu den Fingerabdrücken sind die personenbezogenen Daten und das Foto nicht vor unbefugter Auslesung und Speicherung geschützt. Der Kurierdienst könnte daher ein im Handel verfügbares Lesegerät für Reisepässe und ein dazugehöriges Programm verwenden, um die personenbezogenen Daten und das Foto zu lesen oder zu speichern oder im schlimmsten Fall missbräuchlich zu verwenden.

Die Taskforce empfiehlt den Gemeinden daher, die notwendigen Maßnahmen zu ergreifen, um zu verhindern, dass der Kurierdienst direkten Zugriff auf den Chip der von ihm beförderten Pässe hat. Dies kann z. B. geschehen, indem die Pässe in einem vom Kurierdienst nicht zu öffnenden versiegelten Umschlag an den Antragsteller geliefert werden.

- **Verwendung personenbezogener Daten für die Ausstellung des Reisepasses:**

  Damit dem Antragsteller der Reisepass geliefert werden kann, muss der Kurierdienst in jedem Fall ein Minimum an personenbezogenen Daten verarbeiten und verwenden. Die Taskforce möchte Sie daran erinnern, dass die Verarbeitung personenbezogener Daten den Bestimmungen der Datenschutz-Grundverordnung (DSGVO) und des Gesetzes vom 30. Juli 2018 über den Schutz natürlicher Personen hinsichtlich der Verarbeitung personenbezogener Daten unterliegt (siehe Artikel 2 für die Begriffsbestimmung von "Verarbeitung personenbezogener Daten").

  Die Taskforce möchte die Gemeinden an den Grundsatz der Verhältnismäßigkeit bei der Datenverarbeitung im Hinblick auf den verfolgten Zweck erinnern und empfiehlt ihnen daher:

  - die der Privatgesellschaft zur Verfügung gestellten personenbezogenen Daten so weit wie möglich zu begrenzen (Name, Vorname, Adresse, Telefonnummer, E-Mail-Adresse, ...),
  - die Verwendung der Nationalregisternummer zu vermeiden und
  - der Gesellschaft nicht zu erlauben, die Daten länger aufzubewahren, als es für die Lieferung des Reisepasses an den Empfänger unbedingt notwendig ist.

Da die Gemeinde der Verantwortliche für die der Privatgesellschaft eventuell zur Verfügung gestellten personenbezogenen Daten ist, muss sie in den Vertrag mit dieser Gesellschaft eine

DSGVO-Vereinbarung aufnehmen, in der die Daten, die verwendet werden dürfen, und die Modalitäten für diese Verwendung festgelegt werden.

2.2.4 Rückverfolgbarkeit und Status der Reisepässe

Ein authentischer biometrischer Reisepass ist ein sehr begehrtes Produkt, und wenn er in die falschen Hände gerät, ist Missbrauch nicht ausgeschlossen. Aus diesem Grund müssen die Bewegungen des Reisepasses immer zurückverfolgt werden (auch auf dem Weg zwischen der Gemeinde und dem Antragsteller) und muss der Status des Reisepasses immer aktuell sein und der Wirklichkeit entsprechen.

Folglich sind die nachstehenden Bedingungen zu erfüllen:

- **Rückverfolgung auf dem Weg Gemeinde - Antragsteller:**

  Um das Risiko des Diebstahls, des Verlusts oder der missbräuchlichen Verwendung eines authentischen Reisepasses auf ein Minimum zu reduzieren, ist eine lückenlose Rückverfolgbarkeit des Reisepasses Pflicht. Bis zur Lieferung des Reisepasses an die Gemeinde ist diese Rückverfolgbarkeit durch die Bestimmungen des Vertrags mit dem Reisepasshersteller gewährleistet. Letzterer wurde mehrfach in Bezug auf Sicherheit und Rückverfolgbarkeit geprüft und musste seine Verfahren anpassen, sofern dies als erforderlich erachtet wurde.

Nicht jede von der Gemeinde organisierte Hauslieferung fällt unter die Bestimmungen des Vertrags über die Reisepässe zwischen dem FÖD Auswärtige Angelegenheiten und dem Reisepasshersteller und muss daher im Vertrag zwischen der Gemeinde und dem Kurierdienst geregelt werden. Dieser Vertrag muss die für die **Gewährleistung der Rückverfolgbarkeit notwendigen Bestimmungen** enthalten (z. B. über ein System für die Erfassung und Transportstatusüberwachung, einem "Track-and-trace-System"). Ein vorheriges Audit beim Kurierdienst über die Maßnahmen, die im Hinblick auf die Sicherheit und Rückverfolgbarkeit ergriffen werden, kann ebenfalls sehr dienlich sein.

- **Anpassung des Status des Reisepasses:**

  Es ist sehr wichtig, dass der Status des Reisepasses immer aktuell ist und der Wirklichkeit entspricht, um Missbrauch zu vermeiden (selbst alte abgelaufene Reispässe können noch auf betrügerische Weise genutzt werden). Durch das ***Gesetz vom 10. Februar 2015 über automatisierte Verarbeitungen personenbezogener Daten, die für belgische Pässe und Reisescheine erforderlich sind***, wird zudem keinem anderen Unternehmen als dem Reisepasshersteller der Zugang zur Datenbank für die Reisepässe erlaubt, in der der Status des Reisepasses registriert und fortgeschrieben wird.

Folglich muss die Gemeinde selbst für die korrekte Anpassung des Status des Reisepasses sorgen (z. B. "ausgestellt", "vernichtet", "annulliert"). **Diese Aufgabe darf nicht der Privatgesellschaft anvertraut werden.**

- **Den vorherigen Reisepass abholen & annullieren/vernichten:**

  Da auch alte abgelaufene Reisepässe missbräuchlich verwendet werden können (z. B. unbefugte Nutzung der Daten auf dem Chip, Verwendung leerer Visaseiten zur Erstellung eines gefälschten Reisepasses, ...), ist es wichtig, dass sie tatsächlich eingesammelt und dann **von der Gemeinde selbst** annulliert oder vernichtet werden und nicht vom Kurierdienst.

2.2.5 Identifizierung des Empfängers

Bei der Ausstellung eines Reisepasses am Gemeindeschalter kann der Gemeindebeamte sich vergewissern, dass die Person, die den Reisepass erhält, auch tatsächlich der Antragsteller ist. Selbst wenn ein vom Antragsteller bevollmächtigter Dritter den Reisepass abholt, können die notwendigen Kontrollen am Schalter durchgeführt werden (Vollmachtsformular, Personalausweis des Dritten, ...).

Bei einer Hauslieferung durch einen Kurierdienst ist dies nicht so einfach. Um zu verhindern, dass der Reisepass in falsche Hände gerät, muss Folgendes berücksichtigt werden:

- **Ausarbeitung eines einheitlichen Ausstellungsverfahrens:**

  Der Reisepass darf nur dem **Antragsteller selbst** ausgehändigt werden (Überprüfung seiner Identität auf der Grundlage seines Personalausweises). Handelt es sich um den Reisepass **eines Minderjährigen**, ist das gleiche Verfahren wie am Schalter zu befolgen, d. h. der Reisepass ist gemäß den Vorschriften über die elterliche Autorität einem der beiden Elternteile zu übergeben.

  Für den Fall, dass der Antragsteller zum Zeitpunkt der Hauslieferung nicht anwesend ist, darf das Paket **in keinem Fall** ausgeliefert werden, sondern muss vom Kurierdienst zurückgebracht werden. Bis zu einer möglichen zweiten Lieferung muss der Reisepass an einem sicheren Ort aufbewahrt werden, zu dem nur befugtes Personal entweder der Gemeinde oder der Privatgesellschaft Zugang hat (siehe Nr. 2.2.1 weiter oben).

Es ist ratsam**, alle diese Ausstellungsverfahren in den Vertrag mit dem Kurierdienst aufzunehmen**. Ein vorheriges Audit beim Kurierdienst über die Maßnahmen, die im Hinblick auf die Sicherheit und Rückverfolgbarkeit ergriffen werden, kann ebenfalls sehr dienlich sein.

- **Mögliche Einführung einer Fingerabdruckkontrolle als Identitätskontrolle:**

  Es ist nicht ausgeschlossen, dass in Zukunft ein Abgleich *(Matching*) der Fingerabdrücke des Antragstellers (= Empfänger der Lieferung) mit den Fingerabdrücken auf dem Chip des

ausgestellten Reisepasses eingeführt wird. Dies kann einerseits als Qualitätskontrolle und andererseits im Zusammenhang mit der Bekämpfung von Identitätsbetrug zweckdienlich sein. Ein solches *Matching* wird wahrscheinlich nicht systematisch, aber punktuell im Zweifelsfall auferlegt werden.

Diese Kontrolle ist eine **ausschließliche Zuständigkeit der Exekutive** (= der öffentlichen Behörden) und nicht einer Privatgesellschaft. Zudem gibt es rechtliche und technische Einwände dagegen, dass Fingerabdrücke von einer Privatgesellschaft gelesen werden (Missbrauch sensibler biometrischer Daten, Lesegeräte für Reisepässe müssen einzeln von der Zentralbehörde zertifiziert werden, damit Fingerabdrücke gelesen werden dürfen usw.).

Es ist in jedem Fall ratsam, bei geringsten Zweifeln an der Identität des Empfängers des Reisepasses eine Abholung am Schalter zu verlangen!

2.2.6 Separater Sealbag für Reisepässe, die nach Hause geliefert werden sollen?

Der Reisepasshersteller könnte die für die Hauslieferung bestimmten Reisepässe eventuell in einem separaten Sealbag an die Gemeinde liefern. Allerdings werden hierfür Mehrkosten in Rechnung gestellt, die nicht durch den "Reisepassvertrag" zwischen dem FÖD Auswärtige Angelegenheiten und dem Reisepasshersteller abgedeckt sind.

Interessierte Gemeinden können sich für die diesbezügliche Organisation mit dem Reisepasshersteller in Verbindung setzen; so kann die Fakturierung direkt zwischen der Gemeinde und dem Reisepasshersteller geregelt werden.

2.3 Selbstbedienungsautomat

Bestimmte Gemeinden möchten Identitäts-, Reise- und Aufenthaltsdokumente über einen Selbstbedienungsautomaten ausstellen, sodass der Bürger sein Dokument abholen kann, ohne an einen Schalter gehen zu müssen.

Vorerwähnte Dokumente gelten jedoch als sehr wertvolle Dokumente mit besonders sensiblen personenbezogenen Daten. Sie müssen unter den bestmöglichen Sicherheitsbedingungen ausgestellt werden, wodurch das Risiko von Missbrauch oder Unterschlagung begrenzt wird. In diesem Sinne ist eine Verteilung von Dokumenten über einen Automaten aus folgenden Gründen nicht möglich:

2.3.1 Sicherheitsrisiken

Die Sicherheitsrisiken in Bezug auf diese Art von Automaten, die der Öffentlichkeit rund um die Uhr zugänglich sind, sind beträchtlich:

- gezielter Anreiz für Betrüger und organisierte Banden. Ein außerhalb des Gebäudes eingerichteter Automat wird selbst bei Panzerung immer anfälliger für Diebstahl oder Hackerangriffe sein,
- Risiken für Bürger, die sich zum Automaten begeben,
- Risiken von Vandalismus am Automaten.

2.3.2 Identifizierung des Antragstellers

Die Ausstellung von Dokumenten muss in einem gesicherten Umfeld und unter Aufsicht eines Gemeindebediensteten erfolgen. Der Gemeindebedienstete muss (über das Nationalregister) eine Identitätskontrolle der Person, die das Dokument abholt, vornehmen. Ein Automat ist nicht mit dem Nationalregister, Belpic oder Belpas verbunden und kann daher nicht die notwendigen Überprüfungen der Identität des Inhabers durchführen.

Es ist daher unmöglich, die Person, die das Dokument abholt, eindeutig zu identifizieren.

2.3.3 Verfahrensrechtliche Verpflichtungen

Für die Abholung der verschiedenen Dokumente sind verordnungsrechtliche Verfahren einzuhalten:

- Für **Reisepässe**: Der Status des Reisepasses muss angepasst werden, wenn er dem Inhaber übergeben wird (Status "ausgestellt"), um eine lückenlose Rückverfolgbarkeit des Dokumentes zu gewährleisten. Dies ist umso wichtiger, wenn eine Untersuchung erforderlich ist, falls das Dokument während seiner Gültigkeitsdauer als "gestohlen" oder "verloren" gemeldet wird. Das ersetzte Dokument muss zudem annulliert und dem Gemeindebediensteten zur sofortigen Vernichtung bei der Aushändigung des neuen Dokumentes übergeben werden.
- Für **Personalausweise und Aufenthaltstitel**: Der Status des Dokumentes muss angepasst und die Zertifikate des Ausweises müssen über Belpic aktiviert werden, um eine Online-Identifizierung und eine digitale Signatur zu ermöglichen, damit eine lückenlose Rückverfolgbarkeit des Dokumentes gewährleistet ist. Das ersetzte Dokument muss annulliert und dem Gemeindebediensteten zur sofortigen Vernichtung bei der Aushändigung des neuen Dokumentes übergeben werden. Ein Abgleich der Fingerabdrücke muss zum Zeitpunkt der Ausstellung der Karte ebenfalls durchgeführt werden.

2.4 Mobiles Büro

Einige Gemeinden haben uns mitgeteilt, dass sie mobile Büros für die Beantragung und Ausstellung von Identitäts-, Reise- und Aufenthaltsdokumenten kaufen möchten. Ziel ist es, Anträge von Personen registrieren zu können, die nicht in der Lage sind, sich zur Gemeindeverwaltung zu begeben (z. B. Gefangene, Kranke, ältere Menschen usw.).

Der FÖD Inneres hat ein mobiles Büro entwickelt in Form eines Tablets mit allen Peripheriegeräten und Softwares, die erforderlich sind, um Identitäts- und Aufenthaltsdokumente an anderen Orten als dem Gemeindeschalter zu beantragen und auszustellen.

Die Gemeinden können das mobile Büro von ihrem EDV-Lieferanten beziehen.

3. Schlussfolgerungen

Mit den vorliegenden Empfehlungen will die Taskforce die Gemeinden keinesfalls daran hindern, Dienstleistungsverträge mit Privatgesellschaften zu schließen, um die Dienstleistungen für die Bürger zu verbessern. Tatsächlich ist dies auch das Bestreben der in der Taskforce vertretenen verschiedenen FÖDs.

Diese Dienstleistungsverträge müssen jedoch bestimmte Bedingungen erfüllen, um die Sicherheit der Abläufe zur Beantragung und Ausstellung von Identitäts-, Reise- und Aufenthaltsdokumenten, den Schutz der personenbezogenen Daten der Bürger und die Integrität der Datenbanken der betreffenden FÖDs zu gewährleisten.

Dies liegt im Übrigen im Interesse der Gemeinden und ihrer Bürger.

Daher fordert die Taskforce die Gemeinden auf, den vorliegenden Empfehlungen Folge zu leisten.