EUROPEAN DATA PROTECTION SUPERVISOR

Leitlinien zum Schutz personenbezogener Daten auf von den EU-Organen genutzten mobilen Geräten

Dezember 2015

INHALTSVERZEICHNIS

I. Einleitung 4

I.1. LEITLINIEN 4

I.2. TECHNISCHER HINTERGRUND 5

II. Anwendungsbereich, Methodik und Gliederung der Leitlinien 6

II.1. ANWENDUNGSBEREICH 6

II.2. METHODIK 7

II.3. GLIEDERUNG 8

III. Empfehlungen 8

IV. Sicherheitsmaßnahmen zum Schutz von über mobile Geräte verarbeiteten personenbezogenen Daten 11

IV.1. ORGANISATORISCHE MAßNAHMEN 12

IV.1.1. Lebenszyklusmanagement für das mobile Gerät 12

IV.1.2. Informationssicherheitsstrategie 13

IV.1.3. Schulung 13

IV.1.4. Organisatorische Maßnahmen für BYOD 14

IV.1.5. Sicherheitsverstöße/-vorfälle 14

IV.2. TECHNISCHE MAßNAHMEN 14

IV.2.1. Mobile Device Management („MDM“) 15

IV.2.2. Sonstige technische Maßnahmen 17

V. Datenschutzfragen in Verbindung mit der Verarbeitung personenbezogener Daten über mobile Geräte 19

V.1. EU-ORGANE ALS FÜR DIE VERARBEITUNG UND FÜR DEN DATENSCHUTZ VERANTWORTLICHE GEMÄß VERORDNUNG 19

V.2. SICHERHEITSPFLICHT GEMÄß VERORDNUNG 23

V.3. DATENSCHUTZ-FOLGENABSCHÄTZUNG 24

V.4. MITTEILUNG VON DATENSCHUTZVERLETZUNGEN 24

V.5. SPEZIFISCHES SZENARIO: SEKUNDÄRSPEICHERUNG PERSONENBEZOGENER DATEN ÜBER MOBILE GERÄTE 24

VI. Risiken für personenbezogene Daten bei der Verarbeitung über mobile Geräte 25

VI.1. DATENSCHUTZVERLETZUNGEN BEI GESPEICHERTEN DATEN 27

VI.2. VERARBEITUNG ‚PERSONENBEZOGENER DATEN DRITTER‘ 28

VI.3. ÜBERWACHUNG DER KOMMUNIKATION 28

VI.4. BYOD-SPEZIFISCHE RISIKEN 28

ZUSAMMENFASSUNG

Die Beliebtheit mobiler Geräte ist auf ihre bequeme Nutzung und die zusätzlichen Funktionen zurückzuführen, die sie dem Nutzer in Ergänzung zur effizienten Nutzung von IT-Ressourcen bieten. Der Einsatz mobiler Geräte bringt jedoch spezifische Datenschutzrisiken mit sich, da die Geräte standortunabhängig nutzbar und in vielen Fällen eher auf den Privatanwender als auf eine Nutzung im dienstlichen Kontext zugeschnitten sind.

Ziel dieser Leitlinien ist die Bereitstellung praktischer Empfehlungen und Anweisungen für EU-Organe und -Einrichtungen zu personenbezogenen Daten und zur Nutzung mobiler Geräte im dienstlichen Kontext, um die Einhaltung der für die EU-Organe geltenden Datenschutzverordnung Nr. 45/2001 („Verordnung“) zu gewährleisten.

Werden der Datenschutzbeauftragte und gegebenenfalls die Datenschutzkoordinatoren oder -ansprechpartner frühzeitig und aktiv in den Planungsprozess zur Einführung der Nutzung mobiler Geräte eingebunden, können sie Empfehlungen aussprechen, Verbesserungen vorschlagen und dem Organ allgemein bei der Einhaltung der Verordnung helfen.

Die EU-Organe müssen die Vorteile einer Zulassung der Nutzung mobiler Geräte für spezifische Verarbeitungen (auf Einzelfallbasis) abwägen gegen die möglichen Risiken und Eingriffsintensität. Diese Abschätzung sollte unter Berücksichtigung der zusätzlichen Funktionalitäten und Merkmale der mobilen Geräte sowie der Auswirkungen einer Einführung solcher Geräte auf die Sicherheit der aktuellen IT-Infrastruktur erfolgen.

Bestimmungen zur zulässigen Nutzung im Hinblick auf mobile Geräte sind von grundlegender Bedeutung für die Regelung der Beziehung zwischen EU-Organen und ihren Bediensteten. Wenn die Nutzung eigener Geräte zur Erfüllung dienstlicher Aufgaben (Bring-Your-Own-Device, „BYOD“) gestattet ist, gewinnen solche Bestimmungen zusätzlich an Bedeutung, um die Rechte und Pflichten der EU-Organe und ihrer Bediensteten eindeutig zu definieren.

Das BYOD-Szenario ist immer häufiger anzutreffen, da die mit mobilen Geräten verbundenen Vorteile den EU-Organen und ihren Bediensteten mehr Flexibilität für ihre Arbeitsweise eröffnen. Allerdings bringen sie auch spezifische Risiken für organeigene und private Daten mit sich, die vor der Einführung beurteilt werden müssen. Daher sind spezifische Bestimmungen für die Nutzung eigener Geräte zur Erfüllung dienstlicher Aufgaben erforderlich.

Sicherheit ist eine der Grundvoraussetzungen für den Datenschutz. Um ein angemessenes Schutzniveau sicherzustellen, müssen die EU-Organe einen Risikomanagementprozess einführen, mit dem die mit dem Einsatz mobiler Geräte zur Verarbeitung personenbezogener Daten verbundenen Sicherheitsrisiken bewertet werden. In der Folge müssen die EU-Organe Maßnahmen umsetzen, um den ermittelten Risiken zu begegnen. Diese Maßnahmen sind sowohl organisatorischer (z. B. Einführung von Informationssicherheitsstrategien) als auch technischer Natur (z. B. Mobile Device Management-Lösungen).

Um mobile Geräte ordnungsgemäß zu kontrollieren, unabhängig davon, ob es sich um organeigene oder private Geräte handelt, sollten die Organe dokumentierte Verfahren zum Management des gesamten Lebenszyklus mobiler Geräte einführen unter Berücksichtigung aller auf dem Gerät auszuführenden Vorgänge.

Die vorstehend genannten Maßnahmen sollten die von den EU-Organen verabschiedeten Strategien widerspiegeln unter Beachtung der Grundsätze des eingebauten Datenschutzes und datenschutzfreundlicher Grundeinstellungen. Die Menge der erhobenen und verarbeiteten personenbezogenen Daten sollte auf das notwendige Mindestmaß beschränkt werden (Grundsatz der Datensparsamkeit).

Die vorliegenden Leitlinien beziehen sich auf die mit der Verarbeitung personenbezogener Daten durch EU-Organe über mobile Geräte verbundenen Sicherheitsaspekte, wie in der Verordnung ausgeführt. Wir empfehlen die Lektüre dieses Dokuments in Verbindung mit den Leitlinien des EDSB

„zu personenbezogenen Daten und elektronischer Kommunikation in den EU-Einrichtungen“, die sich auch mit der Überwachung mobiler Geräte durch EU-Organe befassen.

Zwar richten sich diese Leitlinien grundsätzlich an EU-Organe, können aber mit Blick auf den Datenschutz und mobile Geräte auch für andere Personen oder Organisationen hilfreich sein. Verordnung (EG) Nr. 45/2001 entspricht in weiten Teilen der Datenschutzrichtlinie (EG) 95/46, die in das nationale Recht der Mitgliedstaaten sowie jenes von Island, Liechtenstein und Norwegen umgesetzt wurde.

I. Einleitung

I.1. Leitlinien

1 Wenn Bedienstete der EU-Organe, -Einrichtungen oder -Agenturen („EU-Organe“) mobile Geräte für ihren operativen Bedarf einsetzen, kann es sein, dass sie auf diesen Geräten personenbezogene Daten Dritter verarbeiten. Dies könnte jede natürliche Person betreffen, die mit den EU-Organen in beliebiger Weise in Verbindung steht, etwa einen Bürger, der einen der Dienste der EU nutzt, einen Bediensteten, einen Auftragnehmer, einen Bewerber um EU-Fördermittel, einen Pressevertreter oder eine Person in beliebiger sonstiger Funktion. In diesen Situationen ist das jeweilige Organ für die Sicherstellung der Einhaltung der Datenschutzgrundsätze, insbesondere der Verordnung 45/2001[1] (die „Verordnung“) verantwortlich, um das Recht auf Privatsphäre und auf Schutz personenbezogener Daten zu gewährleisten. Die Verantwortung liegt beim jeweiligen EU-Organ, unabhängig von der Herkunft der mobilen Geräte, sprich davon, ob sie der Leitungsebene und Bediensteten mit besonderem dienstlichen Bedarf seitens der EU-Organe bereitgestellt wurden oder ob es sich um **private Geräte** handelt, die die Bediensteten zu dienstlichen Zwecken nutzen dürfen („Bring Your Own Device“ oder „BYOD“).

2 Als unabhängige Aufsichtsbehörde mit Zuständigkeit für die Verarbeitung personenbezogener Daten durch die EU-Organe kann der Europäische Datenschutzbeauftragte (EDSB) unter anderem Leitlinien zu bestimmten Themen im Zusammenhang mit der Verarbeitung personenbezogener Daten herausgeben[2]. Die vorliegenden Leitlinien sind **das Ergebnis eines Prozesses**, in dessen Rahmen eine Konsultation der EU-Organe stattfand.

3 Die Leitlinien richten sich an die behördlichen Datenschutzbeauftragten und Datenschutzkoordinatoren innerhalb jedes EU-Organs, an IT-Bedienstete und IT-Sicherheitsbedienstete und sonstige mit den Prozessen rund um die dienstliche Nutzung mobiler Geräte befasste Verwaltungsstellen sowie an alle Personen, die als für die Verarbeitung zuständige Person Verantwortung für die EU-Organe tragen.

4 Die Leitlinien bieten eine Analyse der allgemeinen Datenschutzrisiken in Verbindung mit der Verarbeitung personenbezogener Daten auf mobilen Geräten sowie Empfehlungen und Informationen zu erprobten Verfahren, die EU-Organe darin unterstützen sollen, ein den Vorgaben der Verordnung entsprechendes Datenschutzniveau zu erreichen. Zwar liegt der Zweck der Leitlinien darin, den EU-Organen die Erfüllung ihrer Pflichten zu erleichtern, jedoch mindert dies keinesfalls die Verantwortung der sie anwendenden EU-Organe. Die EU-Organe bleiben verantwortlich für die ordnungsgemäße Bewertung und Minderung der Risiken in Verbindung mit der Datenverarbeitung. Die Liste der in diesen Leitlinien

[1] Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).
[2] In Ausübung der Befugnisse gemäß Artikel 41 Absatz 2 und Artikel 46 Buchstabe d der Verordnung.

empfohlenen Aktivitäten und Maßnahmen erhebt keinen Anspruch auf Vollständigkeit oder Ausschließlichkeit. Während der EDSB die im Folgenden als „Maßstab“ aufgeführten erprobten Verfahren bei der Beurteilung der Einhaltung von Rechtsvorgaben berücksichtigen wird, sind die EU-Organe dazu aufgerufen, ihre eigene Risikoanalyse durchzuführen und entsprechend geeignete Maßnahmen zu treffen. Ihre Maßnahmen können von den im vorliegenden Dokument vorgestellten abweichen; der EDSB wird die bei einem EU-Organ eingeleiteten Maßnahmen anhand ihrer Vollständigkeit und Effizienz bewerten und nicht anhand der buchstabengetreuen Einhaltung der Leitlinien.

I.2. Technischer Hintergrund

5 Mobile Geräte, insbesondere Smartphones und Tablets, sind im Berufs- und Privatleben allgegenwärtig. Es handelt sich hierbei mittlerweile um ‚Computergeräte zu allgemeinen Zwecken‘, auf denen nahezu jede Anwendung läuft. Neben Sprachanrufen und Textnachrichten bieten sie die Möglichkeit zur Nutzung von Internetdiensten (soziale Netzwerke, Teilen von Inhalten usw.) und umfassen zahlreiche Funktionen, mit denen immer mehr Informationen über die Nutzer erfasst werden, beispielsweise Standortdaten und eine zunehmende Zahl an umweltbezogenen und persönlichen Parametern.

6 Intelligente mobile Geräte nehmen wesentlichen **Einfluss** auf die Arbeitsweise von Organisationen. Zunehmend werden Anwendungen für diese Geräte entwickelt, die feste PC-Arbeitsplätze und Laptops in einigen Einsatzfeldern ersetzen. Zu den Vorteilen zählen eine höhere Mitarbeiterzufriedenheit, Kosteneinsparungen und die Fähigkeit, dem wachsenden Mobilitätsbedarf gerecht zu werden.

7 **Smartphones und Tablets sind nicht die einzigen mobilen Geräte**, die in Organisationen genutzt werden: Mobile Speichermedien wie Speicherkarten, USB-Sticks und externe Festplatten haben ebenfalls große Auswirkungen auf die Datenspeicherung, -übermittlung und -sicherheit. Die ihrer Nutzung innewohnenden **Risiken für die Sicherheit und Privatsphäre** sind hoch und keinesfalls zu vernachlässigen.

8 Diesbezüglich wurden mehrere **kritische Problemfelder** ermittelt:

- Nutzer, die mobile Geräte zu dienstlichen Zwecken der EU-Organe verwenden, verarbeiten häufig personenbezogene Daten, **ohne sich der Tatsache bewusst zu sein,** dass ein Vorgang auf dem mobilen Gerät eine Verarbeitung personenbezogener Daten beinhalten kann, die den Bedingungen und Grenzen der Verordnung unterliegt. Die EU-Organe sind sich möglicherweise der Tatsache nicht bewusst, dass sie – weil die von ihren Beschäftigten in Ausübung ihrer Funktionen ausgeführten Datenverarbeitungen dem EU-Organ zuzuschreiben sind – weiterhin die Haftung für diese Verarbeitungen tragen, selbst wenn diese möglicherweise nur im Rahmen einer Transaktion erfolgen (z. B. Weiterleiten einer E-Mail mit den Kontaktdaten eines neuen Kollegen),

- **‚intelligente'** mobile Geräte ermöglichen die Nutzung von Software-Anwendungen, die mit Internetressourcen interagieren. Sie tauschen über ihre Netzwerkschnittstellen Informationen aus, und dies zuweilen, ohne dass die Nutzer oder Organe sich dessen bewusst sind,
- wenn Bedienstete der EU-Organe ihre eigenen privaten Geräte zu dienstlichen Zwecken nutzen (beispielsweise Zugang und Speicherung von Computerinformationen), ergeben sich zusätzliche datenschutzbezogene Fragestellungen. Der Eigentümer nutzt dasselbe Gerät für seine private Kommunikation und zu anderen Zwecken und installiert hierzu verschiedene Apps seiner Wahl. Die EU-Organe können für private Geräte eine Überprüfung und Kontrolle nicht auf demselben Niveau sicherstellen wie bei eigenen Geräten.

9 Der Grundsatz der **Rechenschaftspflicht** ist im Zusammenhang mit der Nutzung mobiler Geräte von überragender Bedeutung. Dies ist von besonderer Wichtigkeit, weil die klare Definition der einzelnen Verantwortlichkeiten jedes beteiligten Akteurs entsprechend den vielfältigen möglichen Nutzungsfällen sehr kompliziert ist. Eine **enge Zusammenarbeit zwischen den Datenschutzbeauftragten und den Informationssicherheitsbeauftragten** der EU-Organe wird dringend empfohlen.

II. Anwendungsbereich, Methodik und Gliederung der Leitlinien

II.1. Anwendungsbereich

10 Die vorliegenden Leitlinien bieten Empfehlungen für die Einhaltung der Vorschriften zu Privatsphäre und Datenschutz im Zusammenhang mit der Nutzung mobiler Geräte durch Bedienstete der EU-Organe zu dienstlichen Zwecken. Diese Empfehlungen stehen einer separaten oder spezifischen Strategie jedoch nicht entgegen, die die EU-Organe gegebenenfalls angesichts ihrer hochrangigen oder politischen Vertreter in Erwägung ziehen.

11 Diese Leitlinien beziehen sich sowohl auf von den EU-Organen bereitgestellte mobile Geräte als auch auf mobile Geräte im privaten Eigentum ihrer Bediensteten, sofern sie zu dienstlichen Zwecken genutzt werden (BYOD). Der Begriff „**mobile Geräte**" umfasst Telefone, Smartphones, Tablets, Laptops und Netbooks, d. h. alle Geräte, die den Bediensteten ein mobiles Arbeiten ermöglichen, sowie Speichermedien wie externe Festplatten und USB-Sticks. Diese Geräte weisen aufgrund ihrer Standortunabhängigkeit und geringen Größe gemeinsame Risiken auf, wobei sich jedoch die auf ihnen/für sie umsetzbaren Sicherheitsmaßnahmen unterscheiden. Der Schwerpunkt vorliegender Leitlinien liegt auf Smartphones und Tablets. Für sonstige mobile Geräte gelten Unterkategorien der Risiken und empfohlenen Maßnahmen.

12 Während die Nutzung mobiler Geräte zu dienstlichen Zwecken in der Regel viele Fragen im Zusammenhang mit der IT-Sicherheit aufwirft, fallen Risiken die vorhandenen Datenbestände der EU-Organe betreffend nur in den Anwendungsbereich dieser Leitlinien, soweit die IT-Risiken Auswirkungen auf personenbezogene Daten haben.

13 Die vorliegenden Leitlinien beschäftigen sich mit folgenden **Themen**:

- **allgemeine Grundsätze** für die Verarbeitung personenbezogener Daten auf mobilen Geräten durch EU-Organe,
- **Risiken für personenbezogene Daten** bei der Verarbeitung über ein mobiles Gerät,
- **erprobte Verfahren** zum Schutz personenbezogener Daten.

14 Die vorliegenden Leitlinien **befassen sich nicht** mit den folgenden Szenarien und Themen:

- Bedienstete, die **organeigene Geräte**[3] **zu privaten Zwecken** nutzen,
- Nutzung **privater mobiler Geräte** durch Bedienstete **zu rein privaten Zwecken** (selbst wenn das Gerät an den Arbeitsplatz mitgebracht wird),
- Risiken für die Interessen und Besitzstände der EU-Organe mit Ausnahme jener, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen (z. B. Schutz des geistigen Eigentums oder von als vertraulich eingestuften Informationen),
- Verarbeitung der Daten aus der elektronischen Kommunikation zur Ermittlung einer etwaigen unzulässigen Nutzung mobiler Geräte[4] und
- digitale Forensik über mobile Geräte von Bediensteten durch zuständige EU-Organe im Rahmen von Ermittlungen[5].

II.2. Methodik

15 Der Prozess zur Erarbeitung der vorliegenden Leitlinien war derart gestaltet, dass sie als Ergebnis eines **strukturierten offenen Dialogs** mit den EU-Organen bezeichnet werden können. Zentrale Stufen/Elemente dieses Prozesses waren:

- Umfrage vom 21. Juni 2013 als Sachstandserhebung zur Sammlung von Fakten und zwecks Gewinnung eines besseren Verständnisses der Position der EU-Organe zum Thema,
- Workshop vom 19. September 2013 zum Thema auf der Grundlage eines vorab an die Workshop-Teilnehmer versandten Orientierungsdokuments, in dem der EDSB unter anderem die Umfrageergebnisse vorstellte,
- Sichtung erprobter Verfahren im Bereich der Sicherheit von mobilen Geräten,
- Übermittlung des vorläufigen Entwurfs der Leitlinien an die EU-Organe zwecks Feedback und

[3] Da die Nutzung eines mobilen Geräts durch einen Bediensteten **zu privaten Zwecken** keine Verarbeitung durch bzw. im Namen eines EU-Organs darstellt, fällt sie **nicht in den Anwendungsbereich der Verordnung**.
[4] Abgedeckt über die Leitlinien des EDSB „zu personenbezogenen Daten und elektronischer Kommunikation in den EU-Einrichtungen".
[5] ebd.

- endgültige Fertigstellung der Leitlinien unter Berücksichtigung des Feedbacks.

16 Die vorliegenden Leitlinien werden vom EDSB regelmäßig überarbeitet, wobei die EU-Organe über einen Prozess des offenen Dialogs erneut eingebunden werden. Eine erste Überprüfung beginnt zwei Jahre nach Verabschiedung der Leitlinien.

II.3. Gliederung

17 Das vorliegende Dokument ist wie folgt gegliedert:

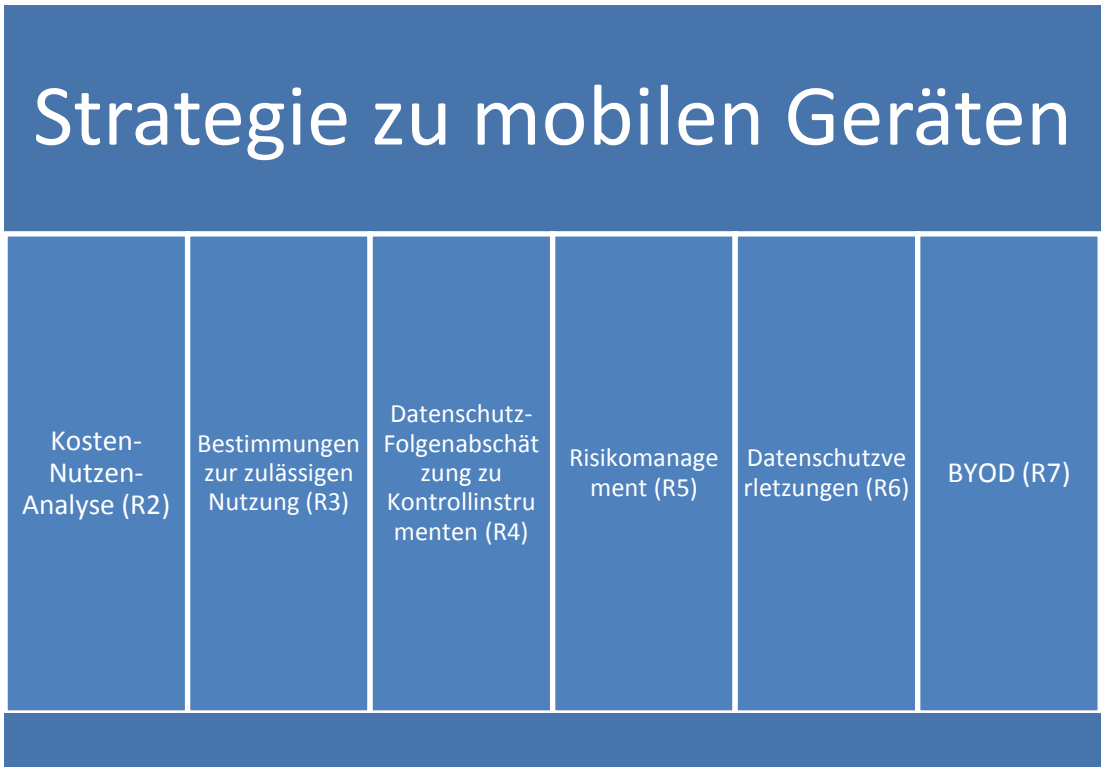
- Abschnitt III *Empfehlungen* enthält die Liste der Empfehlungen, die anhand der in der Verordnung geregelten Pflichten umzusetzen sind. Der Inhalt dieses Abschnitts ist sowohl für die behördlichen Datenschutzbeauftragten/-koordinatoren als auch für die IT-Bediensteten/IT-Sicherheitsbediensteten der EU-Organe am wichtigsten, da er die Themen betrifft, die eine „Strategie zu mobilen Geräten" umfassen sollte.
- Abschnitt IV *Sicherheitsmaßnahmen zum Schutz von über mobile Geräte verarbeiteten personenbezogenen Daten* führt einige auf erprobten Verfahren basierende Sicherheitsmaßnahmen auf, die von den EU-Organen im Umgang mit den Risiken im Zusammenhang mit mobilen Geräten (erläutert in Abschnitt VI) verwendet werden können.
- Abschnitt V *Datenschutzfragen in Verbindung mit der Verarbeitung personenbezogener Daten über mobile Geräte* beinhaltet detailliertere Ausführungen zu den verschiedenen rechtlichen Problemen im Hinblick auf die Nutzung mobiler Geräte laut Definition im Rahmen des vorliegenden Dokuments.
- Abschnitt VI *Risiken für personenbezogene Daten bei der Verarbeitung über* mobile Geräte beschreibt einige der mit mobilen Geräten verbundenen Risiken.

Kursivschrift innerhalb eines Kastens bezeichnet Beispiele und Erläuterungen zum Inhalt des vorstehenden Textes.

Die Abschnitte sind an die Anforderungen der verschiedenen Akteure im Umgang mit der besonderen Problematik mobiler Geräte angepasst: Abschnitt III sollte jeder lesen, da dort die aus der Verordnung resultierenden Pflichten beschrieben werden. Die Abschnitte IV und VI enthalten die wichtigsten technischen Informationen dieser Leitlinien einschließlich Sicherheitsmaßnahmen und Risiken im Zusammenhang mit der Nutzung mobiler Geräte. Abschließend enthält Abschnitt V eine einzelfallbasierte Analyse der Verarbeitung personenbezogener Daten über mobile Geräte in rechtlicher Hinsicht.

III. Empfehlungen

18 Dieser Abschnitt enthält eine Reihe von Empfehlungen, die ein EU-Organ verwenden kann, um die Einhaltung der Vorgaben aus der Verordnung bei der Verarbeitung personenbezogener Daten über mobile Geräte nachzuweisen. Diese Empfehlungen verstehen sich als einzelne Komponenten einer *Strategie zu mobilen Geräten*, wie in folgendem Diagramm dargestellt.



R1: Einbeziehung des behördlichen Datenschutzbeauftragten in alle Aspekte der Einführung und Nutzung mobiler Geräte bei EU-Organen *(siehe Abschnitt V.1)*.

> *Es ist wichtig, dass der behördliche Datenschutzbeauftragte bereits frühzeitig in die Planung zur Einführung der Nutzung des mobilen Geräts eingebunden wird, um sicherzustellen, dass die getroffenen Maßnahmen im Einklang mit der Verordnung stehen.*

R2: **Einzelfallbasierte Abschätzung der Vorteile einer Zulassung der Nutzung mobiler Geräte für spezifische Verarbeitungen unter Berücksichtigung der möglichen Risiken und Eingriffsintensität** *(siehe Abschnitt V.1)*.

> *Diese Abschätzung sollte unter Berücksichtigung der zusätzlichen Funktionalitäten und Merkmale des mobilen Geräts erfolgen, beispielsweise Erweiterung einer Kontaktliste durch Hinzufügen von Fotos für die einzelnen Kontakte mit der Kamera des mobilen Geräts.*
>
> *Sie sollte darüber hinaus die Auswirkungen der Einführung mobiler Geräte auf die Sicherheit der aktuellen IT-Infrastruktur umfassen. Die Einführung unsicherer mobiler Geräte könnte Sicherheitsprobleme in einer IT-Infrastruktur verursachen, die unter der Annahme eingerichtet wurde, dass alle Endgeräte sicher sind und sich Angreifer außerhalb des Netzwerks befinden (siehe Abschnitt V.2).*

R3: Die betreffenden EU-Organe sollten **Bestimmungen zur zulässigen Nutzung** im Hinblick auf mobile Geräte erlassen *(siehe Abschnitt V.1)*. Diese Bestimmungen sollten auch Nutzerpflichten bezüglich der Lebensdauer mobiler Geräte umfassen.

R4: Die verwendeten Überwachungs- und Kontrollinstrumente sollten einer **Datenschutz-Folgenabschätzung** unterzogen werden, um die Sicherheit der mobilen Geräte zu gewährleisten. Die Datenschutz-Folgenabschätzung sollte die wichtigsten Grundsätze und Vorschriften zum Datenschutz gemäß Verordnung berücksichtigen, hierin eingeschlossen Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit, Angabe und Beschränkung des zugrunde liegenden Zwecks, Datenqualität, Datenaufbewahrung, Information der betroffenen Personen und Rechte der betroffenen Personen (Auskunft, Berichtigung, Löschung, Sperrung), Übermittlung von Daten und Vertraulichkeit interner Telekommunikationsnetze oder Endgeräte *(siehe Abschnitt V.3).*

Bei jeder Durchführung einer Datenschutz-Folgenabschätzung für eine bestimmte Verarbeitung ist die Nutzung mobiler Geräte für die betreffende Verarbeitung zu berücksichtigen. Die Folgenabschätzung könnte gemeinsam mit der IT-Sicherheitsrisikobewertung durchgeführt werden; in jedem Fall sollten die verbundenen Sicherheitsrisiken berücksichtigt werden (siehe Abschnitt V.3).

R5: Einrichtung eines ordnungsgemäß dokumentierten **Risikomanagementprozesses**: Es sind geeignete technische und organisatorische Maßnahmen zur Gewährleistung der sicheren Nutzung mobiler Geräte zu treffen. Mit diesen Maßnahmen sollte ein dem betreffenden Risiko entsprechendes Sicherheitsniveau gewährleistet werden unter Berücksichtigung der verfügbaren technischen Lösungen und der Kosten für deren Umsetzung *(siehe Abschnitt V.2).*

Abschnitt VI, Risiken für personenbezogene Daten bei der Verarbeitung über mobile Geräte, enthält eine Beschreibung einiger Risiken im Zusammenhang mit mobilen Geräten. Diese Risiken sollten von den EU-Organen bei ihrer Risikobewertung berücksichtigt werden. In Abschnitt IV, Sicherheitsmaßnahmen zum Schutz von über mobile Geräte verarbeiteten personenbezogenen Daten, sind darüber hinaus einige Sicherheitsmaßnahmen auf der Grundlage erprobter Verfahren aufgeführt. Die EU-Organe sollten diese Maßnahmen als Mittel für den Umgang mit den ermittelten Risiken betrachten.

R6: Verabschiedung interner **Verfahren für den Umgang mit Datenschutzverletzungen**, hierin eingeschlossen Benachrichtigung des behördlichen Datenschutzbeauftragten und des EDSB durch den für die Verarbeitung Verantwortlichen *(siehe Abschnitt V.4),*

R7: Bei Zulässigkeit von **BYOD** sollten die betreffenden EU-Organe:

- vor der Einführung von BYOD in der Organisation zunächst die Risiken für organeigene und private personenbezogene Daten abschätzen *(siehe Abschnitt V.2).*
- eine BYOD-Strategie festlegen *(siehe Abschnitt V.1).*

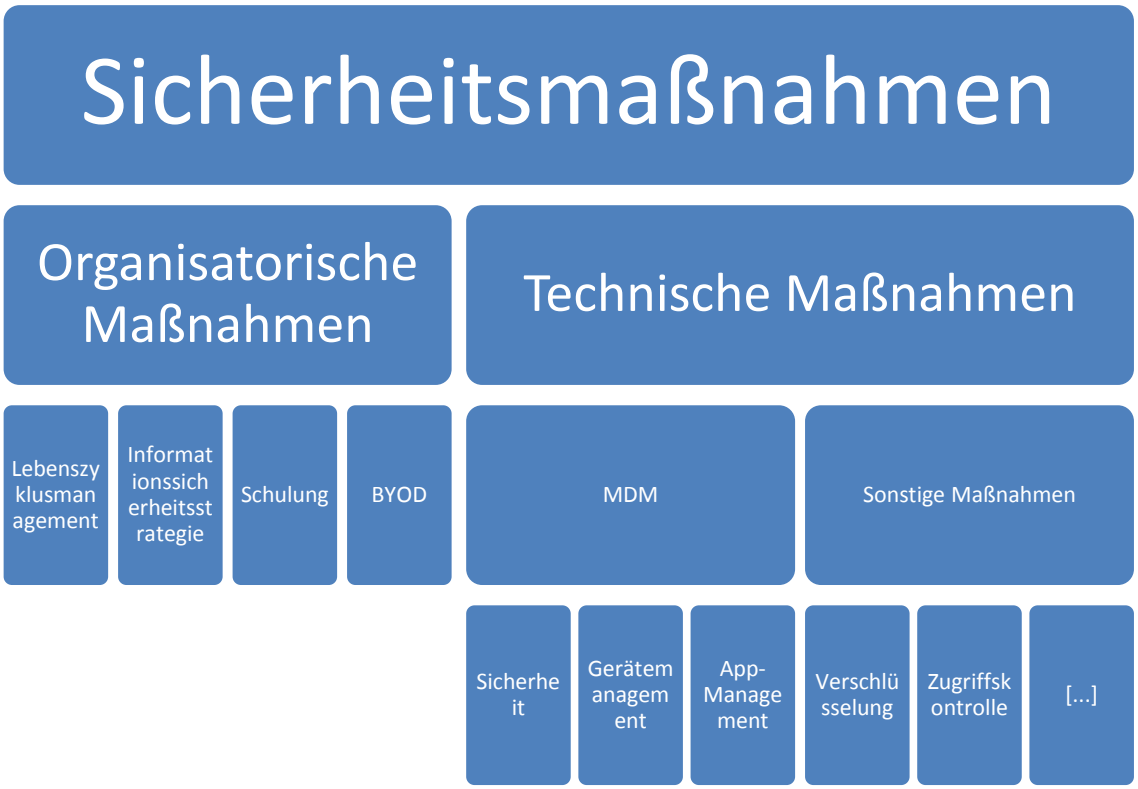
R8: Im Falle des Vorliegens lokaler Kopien personenbezogener Daten auf mobilen Geräten ist es zudem unerlässlich, dass die auf dem jeweiligen mobilen Gerät gespeicherten personenbezogenen Daten ebenfalls berichtigt, gesperrt oder gelöscht werden, wenn die betroffene Person ihr Recht auf Berichtigung unrichtiger oder unvollständiger personenbezogener Daten oder ihr Recht auf Sperrung oder Löschung unrechtmäßig verarbeiteter Daten geltend macht *(siehe Abschnitt V.5).*

R9: Die Nutzung mobiler Geräte an sich ist grundsätzlich kein Grund, Verarbeitungen der Vorabkontrolle durch den EDSB gemäß Artikel 27 der Verordnung zu unterziehen *(siehe Abschnitt V.1).* Die Notwendigkeit, eine bestimmte Verarbeitung einer Vorabkontrolle durch den EDSB zu unterziehen, sollte gemäß Artikel 27 Absatz 2 der Verordnung im Hinblick auf den „Zweck" der Verarbeitung bewertet werden.

IV. Sicherheitsmaßnahmen zum Schutz von über mobile Geräte verarbeiteten personenbezogenen Daten

19 Dieser Abschnitt enthält eine Liste der empfohlenen organisatorischen und technischen Sicherheitsmaßnahmen. Die Liste erhebt keinen Anspruch auf Vollständigkeit, und die EU-Organe können bestimmte Maßnahmen wählen oder alternative Maßnahmen verabschieden, um ihre spezifischen Anforderungen auf der Grundlage ihrer eigenen Risikobewertung und des erforderlichen Sicherheitsniveaus zu erfüllen.

Das folgende Diagramm bietet einen Überblick über diese Sicherheitsmaßnahmen:



IV.1. Organisatorische Maßnahmen

20 Die Einführung mobiler Geräte in einer Organisation bedarf eines umfassenden Instrumentariums von Prozessen, Schulungsplänen, Einbindung der Leitungsebene und Verfahrensweisen für den Umgang mit Vorfällen wie Datenschutzverletzungen.

IV.1.1. Lebenszyklusmanagement für das mobile Gerät

21 Die betreffenden EU-Organe sollten dokumentierte **Verfahren** zum Management des gesamten Lebenszyklus mobiler Geräte einführen.

22 Derartige Verfahren sollten sich auf alle relevanten Phasen des Lebenszyklus eines mobilen Geräts erstrecken (vom Kauf bis zur Entsorgung) unter Berücksichtigung aller auf dem Gerät auszuführenden Vorgänge.

23 Im Rahmen dieses Lebenszyklusmanagements wird das EU-Organ ein **Verzeichnis** von mobilen Geräten erstellen und pflegen müssen, das zu jedem mobilen Gerät mindestens folgende Angaben enthält:

- Gerätebezeichnung und gegebenenfalls SIM-Nummer,
- Gerätestatus (z. B. neu, in Wartung, zugewiesen, zu entsorgen usw.),
- Nutzer, dem das Gerät zugewiesen ist, gegebenenfalls unter Angabe von Anfang und Ende der Zuweisung (z. B. vorübergehend zugewiesene Pool-Geräte),
- Eigentumsverhältnis (organeigen/BYOD).

24 Eine **Geräteentsorgungsstrategie** ist bei mobilen Geräten besonders wichtig. Darin sollten die Pflichten der Nutzer definiert sein. Zudem sollte darin die Speicherung von Informationen zu den zur Entsorgung vermerkten Geräten im Rahmen des gesamten Verzeichnisses mobiler Geräte geregelt sein. Die Wahl der Entsorgungsmethode sollte auf der Grundlage der ermittelten Sicherheitsschwächen jeder Entsorgungsmethode getroffen werden, sodass insbesondere gewährleistet ist, dass alle personenbezogenen Daten bei Entsorgung der Geräte gelöscht sind.

IV.1.2. Informationssicherheitsstrategie

25 Die betreffenden EU-Organe sollten eine Informationssicherheitsstrategie verabschieden, insbesondere eine **Sicherheitsstrategie für mobile Geräte**, sowie eine entsprechende (eindeutige und vollständige) **Datenschutzerklärung**.

> *Die Einbeziehung der Leitung des EU-Organs ist wesentlich für den Erfolg der Strategie, die die Sicherheitsbeschlüsse und -kultur des EU-Organs widerspiegeln sollte. Bei sämtlichen Sicherheitsmaßnahmen sind die Belange des Datenschutzes zu berücksichtigen.*

26 Die behördlichen Sicherheitsbeauftragten und Datenschutzbeauftragten sind frühzeitig in die Erarbeitung der Sicherheitsstrategien und Datenschutzerklärungen einzubeziehen.

IV.1.3. Schulung

27 Ein **Schulungsplan** sollte erstellt werden, um darüber zu informieren, wie sich personenbezogene Daten auf mobilen Geräten schützen lassen, wenn deren Nutzung den Bediensteten gestattet wird.

> *Diese Schulung ist insbesondere von Bedeutung für die Leitungsebene, weil Führungskräfte in der Regel Zugang zu den sensibelsten Daten der Organisation haben. Sie müssen auch auf ihre mögliche persönliche und finanzielle Haftung bei Verstoß gegen die Datenschutzpflichten aufmerksam gemacht werden, ähnlich wie bei ihrer Haftung nach der Haushaltsordnung.*

28 Der Schulungsplan sollte den Maßnahmen des EU-Organs zu mobilen Geräten entsprechend aufgebaut sein und kann die folgenden Szenarien und Themen enthalten:

- grundlegende, sicherheits- und datenschutzrelevante Merkmale mobiler Geräte,
- geschäftsbezogene Anwendungen und Dienste,
- externe Nutzung und Sicherheit (auf Reisen),
- private Nutzung organeigener Geräte,
- BYOD.

29 Der Schulungsplan sollte regelmäßig überprüft und aktualisiert werden.

30 Die Schulung kann für jeden Nutzer eines mobilen Geräts in regelmäßigen Abständen verpflichtend im Rahmen eines Auffrischungskurses zu absolvieren sein.

IV.1.4. Organisatorische Maßnahmen für BYOD

31 Verankerung organisatorischer Strukturen und Prozesse, um sicherzustellen, dass die Vorgaben der Organisation in Bezug auf die Geräte umgesetzt werden (z. B. Beschränkungen in Bezug auf Gerätetyp bzw. -version, Art des Betriebssystems, Einstellungen usw.).

32 Hilfestellung für Nutzer bei der Einstellung der Geräte gemäß den Strategien zu mobilen Geräten im Hinblick auf Sicherheit, Privatsphäre und Datenschutz.

IV.1.5. Sicherheitsverstöße/-vorfälle

33 Es müssen Sicherheitsverfahren eingerichtet sein, um unverzüglich und wirksam auf Sicherheitsvorfälle reagieren zu können (z. B. Verlust oder Diebstahl eines mobilen Geräts). Diese Prozesse sollten die Datenschutzanforderungen berücksichtigen und unter Einbeziehung des behördlichen Datenschutzbeauftragten festgelegt werden.

34 Die Nutzer sollten darüber informiert sein, wie und wo Sicherheitsvorfälle wie Verlust oder Diebstahl zu melden sind. Besondere Aufmerksamkeit gebührt der Tatsache, dass die Nutzer sich zum Zeitpunkt des Vorfalls in der Regel nicht in der Dienststelle befinden werden. Somit sollten adäquate Mittel zur Meldung von Sicherheitsvorfällen vorgesehen werden, über die alle vorstellbaren Szenarien für einen Nutzer abgedeckt sind.

IV.2. Technische Maßnahmen

35 Es gibt mehrere Risiken bezüglich der Verarbeitung personenbezogener Daten. Meist ist die beste und sogar einzige Lösung einiger dieser Probleme die sorgfältige Beurteilung der auf einem mobilen Gerät installierten Anwendungen und die ordnungsgemäße Konfiguration der Betriebssysteme und Anwendungen[6].

36 Das Management und die Konfiguration von Geräten, Betriebssystemen und Anwendungen waren traditionell einmal Aufgabe qualifizierter Bediensteter der IT-Abteilung. Mit der Verbreitung mobiler Geräte, die oftmals im Rahmen von BYOD genutzt werden, wurden einige dieser Aufgaben direkt auf die Nutzer verlagert, die oftmals weder IT-Spezialisten noch Sicherheits-/Datenschutzexperten sind.

37 Zwecks Bewältigung dieser Herausforderung sollten die betreffenden EU-Organe zwei Ansätze kombiniert verwenden:

- Das Verständnis und Bewusstsein der Nutzer für Datenschutzrisiken und mögliche Gegenmaßnahmen stärken[7] und

[6] Weitere Informationen sind zu finden in den in Kürze erscheinenden „Leitlinien zum Schutz von über Internetseiten von EU-Organen und -Einrichtungen verarbeiteten personenbezogenen Daten“ des EDSB sowie in der Stellungnahme der Artikel 29-Datenschutzgruppe vom 27. Februar 2013 zu „Apps auf intelligenten Endgeräten“.

[7] Besteht ein besonderes Risiko für Sicherheitsverstöße, sind die für die Verarbeitung Verantwortlichen gemäß Artikel 35 Absatz 2 der Verordnung verpflichtet, „*die Nutzer über dieses Risiko sowie über mögliche Abhilfen und alternative Kommunikationsmittel*“ zu unterrichten.

- geeignete Lösungen für das „Mobile Device Management“ („MDM“) einsetzen, mit denen durch technische Maßnahmen die Anforderungen hinsichtlich Sicherheit und Datenschutz erfüllt werden.

IV.2.1. Mobile Device Management („MDM“)

38 Mobile Device Management („MDM“)-Lösungen können von der IT-Abteilung des EU-Organs eingesetzt werden, um bestimmte sicherheitsbezogene Aufgaben in Verbindung mit der Konfiguration und dem Management mobiler Geräte zu erfüllen[8]. Diese Option bedeutet für das EU-Organ jedoch erweiterte Verantwortlichkeiten, da derartige Softwarelösungen eine – eher eingreifende – Verarbeitung personenbezogener Daten mit sich bringen (MDM kann z. B. die Echtzeitverfolgung mobiler Geräte erlauben). Die Einhaltung der Datenschutzvorschriften ist daher unverzichtbar.

39 Zu den typischen **Funktionen, die eine MDM-Lösung umfassen sollte**, zählen:

- Sicherheit:
    - Durchsetzung der Verwendung von PIN/Passwort für den Zugriff auf das mobile Gerät, spezifische Anwendungen oder Datencontainer sowie von privaten Schlüsseln,
    - Fernsperrung und -löschung des Geräts (entweder aller auf dem Gerät vorhandenen Daten oder nur organeigener Daten),
    - Erkennung von Konfigurationsänderungen,
    - Beschränkung des Nutzer- und Anwendungszugangs zur Gerätehardware,
    - Beschränkung des Nutzer- und Anwendungszugangs zu nativen Betriebssystemdiensten,
    - Sicherheitsprotokolle und Prüfpfade für das Management von BYOD-Aktivitäten,
    - Sicherung und Wiederherstellung von organeigenen Daten auf dem mobilen Gerät,
    - Compliance-Prüfung vor dem Zugriff auf organeigene Ressourcen,
    - Datenverschlüsselung für auf dem Gerät abgelegte Informationen und bei der Übertragung (Kommunikationsverschlüsselung),
    - Ausstellung und Verwaltung digitaler Zertifikate.
- Gerätemanagement:
    - zentrale Durchsetzung der Sicherheitsstrategie,

[8] Auch wenn in der Vergangenheit MDM-Lösungen zur Nutzungsüberwachung von Mobilgeräten und Abrechnungszwecken genutzt wurden, gehen wir in diesen Leitlinien davon aus, dass sie eine sicherheitsbezogene Zielsetzung verfolgen und betrachten MDM daher nicht als Lösung für eine Nutzungsüberwachung. Siehe diesbezüglich die EDSB-Leitlinien zur elektronischen Kommunikation (Fußnote 4).

- Over-the-air (OTA)-Bereitstellung von Software (Anwendungen und Updates) und Strategieänderungen.

- Anwendungsmanagement:
  - Fernsperrung und -löschung von Anwendungen,
  - Anwendungs-Whitelists und -Blacklists,
  - Stores für Unternehmensanwendungen,
  - sichere Anwendungsbereitstellung mit geeigneten Schutzmechanismen gegen Manipulation/Fälschung,
  - Anwendungsverzeichnis (organeigene und private Anwendungen) pro Gerät,
  - Anwendungssicherheit.

40 Unter Umständen können diese Funktionen über MDM-Systeme nicht auf allen möglichen mobilen Geräten implementiert werden, sondern nur auf einer Untergruppe. Dieser Umstand ist bei der Entscheidung, welche mobilen Geräte zugelassen werden, zu berücksichtigen.

41 Bei Umsetzung einer MDM-Lösung sind folgende Maßnahmen zu treffen:

- Bewertung der Auswirkungen der MDM-Lösung auf den Datenschutz.

> *Im Rahmen dieser Bewertung ist es wichtig zu ermitteln, welche personenbezogenen Daten von der MDM-Lösung erhoben werden und zu welchem Zweck, wo und wie lange sie gespeichert werden und wer Zugang zu den Daten und Protokollfunktionen hat. Das EU-Organ sollte prüfen, ob diese Informationen für den vorgesehenen Zweck unbedingt erforderlich sind oder ob es weniger eingreifende Lösungen gibt.*

- Information der Nutzer über die Bestimmungen zur zulässigen Nutzung der MDM-Lösung auf ihrem mobilen Gerät, zur Art der über MDM erhobenen Daten und zum Zweck der Datenerhebung.

> *Die vom EU-Organ umgesetzte MDM-Lösung, mit der die Sicherheit der von Bediensteten auf ihren eigenen Geräten verarbeiteten organeigenen Daten gewährleistet werden soll, kann eine intensivere Überwachung der Bediensteten bei der Arbeit durch das EU-Organ mit sich bringen. Diese Überwachung könnte beispielsweise die Aufzeichnung der geografischen Standortdaten des Mobilgeräts oder die Kontrolle des Internetverkehrs auf dem Gerät umfassen.*

- Beschränkung des Zugangs zur Administratorkonsole der MDM-Lösung auf der Grundlage des Prinzips der geringsten Rechte gemäß dem Grundsatz „Kenntnis nur wenn nötig“[9].

[9] *Kenntnis nur wenn nötig*: Der Zugang des Nutzers zu den Informationen muss zur Erfüllung der Aufgaben des Nutzers erforderlich sein. *Geringste Rechte*: Die Rechte eines Nutzers hinsichtlich bestimmter Informationen (Lesen, Schreiben usw.) müssen die Mindestrechte sein, die zur Erfüllung der Aufgaben des Nutzers erforderlich sind.

- Bewertung der Abdeckung der MDM-Lösung unter Berücksichtigung des kompletten Bestands an mobilen Geräten und anderer Datenquellen wie Anwendungen oder Netzwerkprotokolle.

IV.2.2. Sonstige technische Maßnahmen

42 Eine MDM-Lösung allein wird nicht alle Risiken abdecken können, die mit der Nutzung mobiler Geräte verbunden sind. Die folgende Liste umfasst mögliche technische Maßnahmen, die in Abhängigkeit von den spezifischen Risiken des einzelnen EU-Organs umgesetzt werden können. Einige dieser Maßnahmen würden mit Blick auf ihre Umsetzung von einer MDM-Lösung profitieren, auch wenn sie eine solche für ihre Funktion nicht zwingend erfordern. Diese Sicherheitsmaßnahmen sollten auch unter Berücksichtigung spezifischer Geräte betrachtet werden: Eine Verschlüsselung ist für tragbare Speichermedien, z. B. USB-Sticks, möglich, nicht jedoch eine Anti-Malware-Software, zumindest nicht auf dem USB-Stick selbst.

43 T1: Konzeption, Umsetzung und Wartung einer Sandbox-, Kompartimentierungs- oder Virtualisierungslösung zur Trennung privater und organeigener Daten.

> *Eine Sandbox bietet eine eng kontrollierte Umgebung auf einem mobilen Gerät, in der Anwendungen laufen. Mittels Kompartimentierung wird ein verschlüsselter Datenspeicher auf einem mobilen Gerät eingerichtet. Für den Zugriff auf die in einem geschlossenen Kompartiment gespeicherten Daten ist eine Authentifizierung erforderlich, die zusätzlich zu anderen auf dem mobilen Gerät angewendeten Authentifizierungssystemen läuft.*

44 T2: Entwicklung, Umsetzung und Test einer Verschlüsselungslösung, über die sichergestellt werden soll, dass auf mobilen Geräten (oder zumindest im organeigenen Kompartiment des Geräts, sofern eine Kompartimentierung/MDM-Lösung zum Einsatz kommt) gespeicherte personenbezogene Daten verschlüsselt werden.

45 Diese Lösung kann folgende Merkmale umfassen:

- Erfordernis einer vollständigen Festplattenverschlüsselung für alle Geräte und einer zusätzlichen Verschlüsselung für sichere Anwendungscontainer,
- Erfordernis, nur Standard-Verschlüsselungsalgorithmen zu verwenden,
- die Länge der Verschlüsselungscodes muss den Sicherheitsanforderungen entsprechen.

46 T3: Entwicklung, Umsetzung und Test einer Backup-Lösung zur Sicherung der Verfügbarkeit von nur auf dem mobilen Gerät gespeicherten Daten.

> *In den meisten Fällen ist das mobile Gerät nicht der Hauptspeicherort für dienstliche Daten und die Gerätekonfiguration erfolgt über einen zentralen Datenspeicher, was Backups überflüssig macht. Andererseits können personenbezogene Daten (wie Kontaktdaten) nur auf dem mobilen Gerät gespeichert sein und daher einer Sicherung bedürfen.*

47 T4: Konzeption und Umsetzung einer geeigneten Benutzerauthentifizierung für das mobile Gerät einschließlich PIN und Passwörter zur Entsperrung des mobilen Geräts.

Für Benutzer mit Zugang zu sensiblen Daten kann neben PIN/Passwort ein zweiter Authentifizierungsfaktor eingerichtet werden.

Das mobile Gerät sollte nach einer voreingestellten Anzahl nicht erfolgreicher PIN-/Passworteingaben gesperrt und/oder gelöscht werden.

48 T5: Deaktivierung nicht erforderlicher Funktionen.

z. B. standardmäßige Deaktivierung unnötiger oder risikobehafteter Funktionen wie GPS, Nahfeldkommunikation (NFC), Bluetooth usw. Durch die Deaktivierung unnötiger Funktionen wird das mobile Gerät sicherer, da die Angriffsfläche für eine Manipulation des Geräts durch Angreifer verringert wird und das mobile Gerät aufgrund der geringeren Zahl an Komponenten leichter zu warten ist.

49 T6: Umsetzung einer sicheren und die Privatsphäre schützenden Standardkonfiguration für mobile Geräte und Anwendungen.

z. B. automatische Sperrung des mobilen Geräts bei Inaktivität

50 T7: Sicherstellung zeitnaher Softwareupdates des mobilen Geräts und der installierten Anwendungen (mit und ohne MDM-Lösung).

51 T8: Der Zugang zu den internen Netzwerken der EU-Organe sollte erst nach Validierung der Netzwerkverbindung von einem mobilen Gerät anhand des organeigenen Verzeichnisses und der organeigenen Autorisierungen gewährt werden.

Gerätespezifische und/oder nutzerspezifische digitale Zertifikate können verwendet werden, um das mobile Gerät/den Nutzer zu identifizieren und authentifizieren, bevor Zugang zum Netzwerk gewährt wird.

Für Verbindungen zu sensiblen Anwendungen oder Informationen kann eine Zwei-Faktor-Authentifizierung umgesetzt werden.

52 T9: Ausschließliche Zulassung von verschlüsseltem Datenverkehr zwischen den mobilen Geräten und dem internen Netzwerk des EU-Organs.

Nutzer sollten sich der Tatsache bewusst sein, dass VPN (Virtual Private Networks), die für die Verschlüsselung des Datenverkehrs zwischen dem mobilen Gerät und dem internen Netzwerk zum Einsatz kommen, den gesamten Datenverkehr einschließlich privater Kommunikation über das IT-Netzwerk des EU-Organs umleiten können.

53 T10: Einsatz branchenüblicher Firewalls und Anti-Malware-Anwendungen auf den mobilen Geräten und Sperrung des Zugangs zum organeigenen Netzwerk für Geräte ohne derartige Firewalls und Anwendungen und/oder mit einer veralteten Konfiguration. Sowohl die Firewall als auch die Anti-Malware-Anwendung sollten regelmäßig aktualisiert werden (automatisch oder manuell, über eine MDM-Lösung oder direkt über den Anbieter der Firewall oder Anti-Malware-Anwendung).

54 T11: Gemäß den Bestimmungen zur zulässigen Nutzung Sperrung der Nutzung von Drittanwendungen für die Verarbeitung personenbezogener Daten des EU-Organs,

sofern nicht in den Strategien des Organs vorgesehen sowie nach geeigneter Beurteilung der bestehenden Risiken für personenbezogene Daten.

V. Datenschutzfragen in Verbindung mit der Verarbeitung personenbezogener Daten über mobile Geräte

V.1. EU-Organe als für die Verarbeitung und für den Datenschutz Verantwortliche gemäß Verordnung

55 Im Zusammenhang mit der Verarbeitung über mobile Geräte ist es besonders wichtig darauf hinzuweisen, dass es sich bei personenbezogenen Daten[10] um alle Informationen über eine bestimmte oder bestimmbare natürliche Person handelt: Hierzu zählen nicht nur Daten über die Bediensteten von EU-Organen, sondern auch über natürliche Personen, die nicht in einem Arbeitsverhältnis mit EU-Organen oder -Agenturen stehen.

> *Mobile Geräte können beispielsweise genutzt werden, um mobil auf das organeigene E-Mail-Konto des Nutzers zuzugreifen oder auf eine Datenbank mit personenbezogenen Daten sowie für den Download oder die Synchronisierung dieser Daten auf dem mobilen Gerät. Berufsbezogene mobile Anwendungen können auf dem Gerät installiert werden, um auf Datenbanken oder Webportale zuzugreifen, wo ebenfalls verschiedene Kategorien personenbezogener Daten verfügbar sein können (z. B. Personalmanagementsystem).*
>
> *Die fraglichen personenbezogenen Daten können somit Namen, E-Mail-Adressen, Telefonnummern, Datenverkehrs- und Standortdaten, IP-Adressen und Cookies umfassen, sofern über diese eine natürliche Person bestimmt werden kann. Ebenfalls zu berücksichtigen ist die Tatsache, dass personenbezogene Daten in jeder Form verarbeitet werden können, beispielsweise in einer E-Mail, die personenbezogene Daten enthält, sowie mit jeder Technologie, hierin eingeschlossen Internetprotokolle. Selbst im einfachsten Fall, beispielsweise wenn das Gerät nur für die Telefonkommunikation und SMS genutzt wird, werden die Verkehrs- und Kontaktdaten der Telefonnutzer und ihrer Kommunikationspartner verarbeitet. Darüber hinaus verwenden Smartphones und Tablets eine Reihe von Technologien, mit denen Einzelpersonen bestimmt und in Bezug auf ihren physischen Standort sowie ihre Nutzung von Geräten und Anwendungen (standortbasierte Dienste, die auf Mobiltelefonen und Tablets verfügbar sind, erheben Standortdaten, über die Dritte den genauen Standort der Nutzer bestimmen können) verfolgt werden können. Ferner können personenbezogene Daten Dritter (genauer von Personen, die nicht in einem Arbeitsverhältnis mit EU-Organen stehen) in Nachrichten und gespeicherten Anrufen enthalten sein, z. B. in einem Voicemail-System.*

56 Die EU-Organe müssen personenbezogene Daten auch zum Management der mobilen Geräte selbst erheben und verarbeiten und werden oft auch ad-hoc Software auf diesen installieren. Dies ist der Fall bei der Installation sogenannter „Mobile Device Management"-Lösungen (MDM), über die die Geräte um Funktionen zur

[10] Gemäß Definition in Artikel 2 Buchstabe a der Verordnung. Siehe auch Stellungnahme der Artikel 29-Datenschutzgruppe 4/2007 zum Begriff „personenbezogene Daten" vom 20. Juni.

sicherheitsbezogenen Datenerhebung und Geräteintervention ergänzt werden, indem sie mit dedizierten zentralen Kontrollservern verbunden werden.

57 Wenn ein Bediensteter eines EU-Organs ein mobiles Gerät für dienstliche Aufgaben auf Anweisung des EU-Organs nutzt, ist dieses Organ der für die Verarbeitung Verantwortliche, da es den Zweck und die Art der Verarbeitung der personenbezogenen Daten bestimmt. Die über die mobilen Geräte durchgeführte Verarbeitung fällt somit in den Anwendungsbereich der Verordnung.[11]

58 Auch im ‚BYOD'-Szenario, das aufgrund der geringeren Kontrolle des EU-Organs über das mobile Gerät problematischer ist als das Szenario mit organeigenen Geräten, ist das EU-Organ weiterhin verantwortlich dafür, alle erforderlichen Maßnahmen zu ergreifen, um seine Pflichten aus der Verordnung zu erfüllen und einen internen Mechanismus zum Nachweis der Erfüllung einzurichten.

59 Die EU-Organe sollten darauf achten, dass die Verarbeitung über mobile Geräte dieselben Anforderungen und Grundsätze erfüllen muss wie die Verarbeitung in der ‚herkömmlichen' Desktop-Umgebung.

60 Ein Bediensteter eines EU-Organs, der sein eigenes Gerät zur Erfüllung dienstlicher Aufgaben nutzt (BYOD), ist verpflichtet, die vom EU-Organ für diesen Kontext eigens verabschiedeten Strategien umzusetzen.

61 Entsprechend dem Grundsatz der Rechenschaftspflicht ist es wichtig, dass der behördliche Datenschutzbeauftragte bereits in der frühen Phase der Planung und des Managements der Datenverarbeitung über mobile Geräte eingebunden ist, um sicherzustellen, dass die zur Minderung oder Behebung der Datenschutzrisiken ergriffenen Maßnahmen geeignet sind und der Verordnung entsprechen.

62 Die folgenden **Szenarien** können daher als Hauptbeispiele für die Verarbeitung personenbezogener Daten mittels Nutzung mobiler Geräte betrachtet werden:

- Datenverarbeitung durch EU-Organe (oder ihre Bedienstete) über mobile Geräte (organeigene Geräte oder gemäß BYOD-Szenario) als Instrument für Datenverarbeitungen, die mit jenen vergleichbar sind, die bereits von EU-Organen in der herkömmlichen IT-Umgebung (‚Desktop'-Umgebung) durchgeführt werden
- EU-organseitige Überwachung der Nutzung der mobilen Geräte durch Bedienstete[12]
- Verarbeitung personenbezogener Daten im Kontext der Umsetzung von MDM-Lösungen

[11] Als Beispiel für die Anwendung der Verordnung kann angeführt werden, dass wenn – im Rahmen dieses Szenarios – das mobile Gerät zur Aufnahme von Videos oder Fotos verwendet wird, das EU-Organ die in den thematischen Leitlinien des EDSB zu **Videoüberwachung** unter Punkt 2.3.1 „Erstrecken sich die Leitlinien auf andere Systeme als Videokameraüberwachungssysteme („CCTV-Systeme")? beschriebenen Fragestellungen beachten muss: „(…) Doch auch die Verwendung anderer fester oder **transportabler** elektronischer Geräte oder Systeme fällt in den Geltungsbereich der Leitlinien, sofern diese in der Lage sind, Bilddaten zu erfassen" (Hervorhebung in Fettschrift eingefügt).

[12] Dieses Szenario fällt nicht in den Anwendungsbereich dieser Leitlinien und wird in den EDSB-Leitlinien zur elektronischen Kommunikation (Fußnote 4) behandelt.

63 In allen vorstehend genannten Fällen kommt die Verordnung zur Anwendung.

64 In Erwägungsgrund 12 der Verordnung ist gefordert: „Die kohärente, homogene Anwendung der Bestimmungen für den Schutz der Grundrechte und Grundfreiheiten von Personen bei der Verarbeitung personenbezogener Daten sollte in der gesamten Gemeinschaft gewährleistet sein." Dies schließt die Datenschutzrichtlinie für elektronische Kommunikation ein (Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation). Unbeschadet einzelfallbezogener Bestimmungen bilden diese Vorschriften eine Bezugsgrundlage für die EU-Organe. Diesbezüglich ist es von wesentlicher Bedeutung, Folgendes zu berücksichtigen: „Im Fall einer Verletzung des Schutzes personenbezogener Daten benachrichtigt der Betreiber der öffentlich zugänglichen elektronischen Kommunikationsdienste unverzüglich die zuständige nationale Behörde von der Verletzung. Ist anzunehmen, dass durch die Verletzung personenbezogener Daten die personenbezogenen Daten, oder Teilnehmer oder Personen in ihrer Privatsphäre, beeinträchtigt werden, so benachrichtigt der Betreiber auch den Teilnehmer bzw. die Person unverzüglich von der Verletzung." – Artikel 4 Absatz 3 der Richtlinie 2002/58 (geändert durch Richtlinie 2009/136/EG). Diese Regeln sind nicht direkt auf EU-Organe und -Einrichtungen anwendbar, können jedoch als erprobte Verfahren betrachtet werden (siehe Punkt V.4 unten).

65 In der Verordnung sind die Bedingungen festgeschrieben, unter denen eine rechtmäßige Verarbeitung personenbezogener Daten erfolgen kann. Der für die Verarbeitung Verantwortliche[13] muss sicherstellen, dass Bedienstete mobile Geräte nicht für eine Verarbeitung nutzen, für die keine **Rechtsgrundlage**[14] besteht.

66 Die **Notwendigkeit und Verhältnismäßigkeit** der Verarbeitung personenbezogener Daten über mobile Geräte erfordert, dass die EU-Organe eine einzelfallbasierte Abschätzung der Vorteile einer Zulassung der Nutzung mobiler Geräte unter Berücksichtigung der möglichen Risiken und Eingriffsintensität vornehmen. Diese Abschätzung sollte unter Berücksichtigung der zusätzlichen Funktionalitäten und Merkmale des mobilen Geräts erfolgen, beispielsweise Erweiterung einer Kontaktliste durch Hinzufügen von Fotos, die mit der Kamera des mobilen Geräts aufgenommen wurden.

67 Die Nutzer der mobilen Geräte müssen über die aufgrund ihrer Nutzung mobiler Geräte erfolgende Datenverarbeitung **informiert**[15] werden, unabhängig davon, ob es sich um organeigene oder private Geräte handelt. Dies gilt umso mehr, wenn personenbezogene Daten zum Management der mobilen Geräte selbst erhoben und

[13] Wie in Abschnitt V.1 angegeben, ist das EU-Organ der für die Verarbeitung Verantwortliche, da es den Zweck und die Art der Verarbeitung der personenbezogenen Daten bestimmt.
[14] Gemäß Definition in Artikel 5 der Verordnung. In vielen Fällen wird die Verarbeitung auf Artikel 5 Buchstabe a basieren, hierin eingeschlossen eine Verarbeitung, die für die Verwaltung und das Funktionieren der Einrichtung erforderlich ist (Erwägungsgrund 27).
[15] Artikel 11 und/oder 12 der Verordnung.

verarbeitet werden. Die EU-Organe sollten Bestimmungen zur zulässigen Nutzung im Hinblick auf mobile Geräte erlassen, die Folgendes umfassen sollten:

- eindeutige Definition der vom EU-Organ zugelassenen Nutzungen der mobilen Geräte,
- Folgen eines Missbrauchs mobiler Ressourcen,
- welche organeigenen und personenbezogenen Daten auf mobilen Geräten gespeichert und an diese übermittelt werden dürfen,
- Typ und Version der zulässigen mobilen Geräte und Betriebssysteme,
- welche Anwendungen installiert und genutzt werden dürfen,
- Bestimmungen des EU-Organs zur Nutzung von Cloud-Diensten,
- Bestimmungen zu Rückgabe und Entsorgung,
- eindeutige Beschreibung der Verantwortlichkeiten des Nutzers und des EU-Organs,
- unter welchen Bedingungen die Überwachung der Nutzung mobiler Geräte durch Bedienstete des EU-Organs zulässig ist, und
- Informationen zu den personenbezogenen Daten, die der Nutzer über sein mobiles Gerät erheben und verarbeiten darf.

68 Die Bestimmungen zur zulässigen Nutzung sollten von den Nutzern formell angenommen werden, bevor sie mobile Geräte nutzen. Bei Änderungen der Bestimmungen zur zulässigen Nutzung sind die neuen Bestimmungen den Nutzern unverzüglich zu übermitteln und müssen erneut von ihnen angenommen werden.

69 Für das BYOD-Szenario sollten die BYOD-Bestimmungen für alle potenziellen BYOD-Nutzer problemlos verfügbar sein, bevor sie sich für oder gegen eine Nutzung privater mobiler Geräte zu dienstlichen Zwecken entscheiden. Diese Bestimmungen sollten zusätzlich zu den Bestimmungen zur zulässigen Nutzung für alle mobilen Geräte als Voraussetzung für die BYOD-Zulassung eine ausdrückliche Annahme erfordern sowie eine ausdrückliche Genehmigung des Nutzers im Hinblick auf die Systemverwaltung und -überwachung von BYOD-Geräten.

70 Die Konfiguration des mobilen Geräts sollte die Regeln widerspiegeln („berücksichtigen“) (unter Beachtung der Grundsätze eines eingebauten Datenschutzes, datenschutzfreundlicher Grundeinstellungen und der Datensparsamkeit). Zur Umsetzung des Grundsatzes der Angabe/Beschränkung des zugrundeliegenden Zwecks ist es wichtig, eine ‚schleichende Ausweitung der Zweckbestimmung‘ (Erhebung und Verarbeitung für nicht zulässige sekundäre Zwecke) zu vermeiden, beispielsweise mittels Ausschluss der Installation von für die dienstlichen Aufgaben nicht erforderlichen Apps und Trennung von dienstlichen und privaten Daten.

71 Unabhängig von der für eine spezifische Verarbeitung anwendbaren Rechtsgrundlage ist es wichtig, zuerst den Zweck der Datenverarbeitung zu betrachten und nicht das genutzte technische Gerät: Die **Nutzung mobiler Geräte an sich ist grundsätzlich kein Grund, Verarbeitungen der vorherigen Prüfung durch den EDSB gemäß Artikel 27 der Verordnung zu unterziehen**. Die Notwendigkeit, eine bestimmte Verarbeitung der Vorabkontrolle durch den EDSB zu unterziehen, sollte im Hinblick auf den „Zweck" der Verarbeitung bewertet werden gemäß Artikel 27 Absatz 2 der Verordnung.

V.2. Sicherheitspflicht gemäß Verordnung

72 Die für den Datenschutz Verantwortlichen müssen geeignete technische und organisatorische Maßnahmen zur Gewährleistung der sicheren Nutzung mobiler Geräte treffen. Diese Maßnahmen sollten geeignet sein, ein Schutzniveau zu gewährleisten, das den bestehenden Risiken angemessen ist, und dies unter Berücksichtigung des Standes der Technik und der bei der Durchführung entstehenden Kosten[16].

73 Dies impliziert, dass die für den Datenschutz Verantwortlichen einen **datenschutzbezogenen Risikomanagementprozess** umsetzen müssen, der den etablierten Grundsätzen erprobter Verfahren entspricht. Der erste Schritt in diesem Prozess ist eine Bewertung der Risiken, die auch eine Analyse der Nutzung mobiler Geräte umfassen sollte. Diese Bewertung hilft bei der Ermittlung der größten Sicherheitsrisiken und bildet die Grundlage für die Auswahl der geeigneten Kontrollen, die eingeführt werden müssen, um die Risiken auf ein für die Leitungsebene annehmbares Niveau zu reduzieren. Zum Risikomanagementprozess gehört auch eine regelmäßige Überprüfung der Risikobewertung sowie der Angemessenheit von Garantien und Kontrollen.

74 Der Risikomanagementprozess muss als Strategie des EU-Organs ordnungsgemäß dokumentiert werden. Er muss regelmäßig überarbeitet werden, um sicherzustellen, dass er seine Wirksamkeit behält und sich an neue und sich wandelnde Ziele der Organisation anpasst. An diesem Prozess (und insbesondere an der Analyse von Sicherheitsrisiken) beteiligte Bedienstete sollten sich nicht nur auf die Sicherheit innerhalb des EU-Organs konzentrieren. Vertreter der ‚Kerntätigkeit' (HR, Kern-/operative Tätigkeiten) und der behördliche Datenschutzbeauftragte sollten ebenfalls in die Gespräche eingebunden werden, um sicherzustellen, dass bei der Analyse die Auswirkungen aller Aspekte der Tätigkeit Berücksichtigung finden.

75 Den betroffenen Bediensteten sollten die zentralen Ergebnisse des datenschutzbezogenen Risikomanagementprozesses und die bestehenden Sicherheitsrisiken in vollem Umfang mitgeteilt werden. Für die Leitungsebene und die zentralen Akteure können detaillierte Informationen zu den Ergebnissen dieses Prozesses hilfreich sein.

[16] Gemäß Artikel 22 der Verordnung.

V.3. Datenschutz-Folgenabschätzung

76 Der EDSB empfiehlt, bei jeder Durchführung einer Datenschutz-Folgenabschätzung durch EU-Organe die Nutzung mobiler Geräte zu berücksichtigen. Die Datenschutz-Folgenabschätzung sollte insbesondere gemeinsam mit der IT-Sicherheitsrisikobewertung durchgeführt werden; in jedem Fall sollten die verbundenen Sicherheitsrisiken berücksichtigt werden.

77 Die Datenschutz-Folgenabschätzung sollte sich insbesondere auf die Überwachungs- und Kontrollinstrumente beziehen, die eingesetzt werden, um die Sicherheit der mobilen Geräte sicherzustellen. Die Folgenabschätzung sollte die wichtigsten Grundsätze und Vorschriften zum Datenschutz gemäß Verordnung berücksichtigen, einschließlich der Grundsätze von Rechtmäßigkeit, Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung, Angabe und Beschränkung des zugrunde liegenden Zwecks, Datenqualität, Vorratsdatenspeicherung, Information der betroffenen Personen und Rechte der betroffenen Personen (Auskunft, Berichtigung, Löschung, Sperrung) sowie Datenübermittlungen.

V.4. Mitteilung von Datenschutzverletzungen

78 Der EDSB empfiehlt den EU-Organen den Beschluss interner Verfahren zum Umgang mit Datenschutzverletzungen, die insbesondere die Benachrichtigung des behördlichen Datenschutzbeauftragten durch den für die Verarbeitung Verantwortlichen vorsehen.

> *Bei Verlust oder Diebstahl des mobilen Geräts und damit verbundener Verletzung des Schutzes personenbezogener Daten beispielsweise sollte der Bedienstete den Vorfall intern entsprechend den Bestimmungen des EU-Organs zum Umgang mit Sicherheits- und Datenschutzverletzungen melden. Der behördliche Datenschutzbeauftragte sollte die Verletzung und die als Reaktion getroffenen Maßnahmen analysieren und dokumentieren, damit eine zukünftige Bewertung und Prüfung erfolgen können und entschieden werden kann, ob der EDSB informiert werden sollte. Die Reaktion des EDSB auf derartige Datenschutzverletzungen ist natürlich von einer Reihe von Faktoren abhängig, unter anderem vom Schweregrad der Verletzung, Art und Umfang der betroffenen Daten, Anzahl der betroffenen Personen, Ort der Datenempfänger usw.*

V.5. Spezifisches Szenario: Sekundärspeicherung personenbezogener Daten über mobile Geräte

79 Bei der Verarbeitung personenbezogener Daten über ein mobiles Gerät kann der Nutzer Kopien personenbezogener Daten aus zentralen Informationssystemen auf dem Gerät speichern. Diese ‚Sekundärspeicherung' kann Probleme mit sich bringen bezüglich der Datenqualität, Ausübung des Rechts der betroffenen Person auf Berichtigung, Sperrung und Löschung sowie Einhaltung der zulässigen Dauer der Vorratsdatenspeicherung. Es kann vorkommen, dass diese auf dem mobilen Gerät gespeicherten Daten nicht mehr korrekt oder aktuell sind, wohingegen die Daten im zentralen Speichersystem des EU-Organs aktualisiert wurden. Die Risiken für das

EU-Organ steigen aufgrund dieser möglicherweise mangelnden Kenntnis von Verarbeitungen, die über ein mobiles Gerät stattfinden.

> *Ein Bediensteter der Personalabteilung eines EU-Organs könnte beispielsweise auf sein mobiles Gerät einen E-Mail-Anhang herunterladen, der personenbezogene Daten eines Kollegen enthält.*
>
> *Ebenso könnte ein Nutzer eine Anwendung einsetzen, die die auf seinem mobilen Gerät gespeicherten Daten ohne sein Wissen in der Cloud repliziert. Dieses Szenario birgt weitere Risiken für die vertrauliche Behandlung verarbeiteter personenbezogener Daten.*

80 Umfasst die vom EU-Organ vorgesehene Verarbeitung lokale Kopien personenbezogener Daten auf mobilen Geräten, ist es zudem unerlässlich, dass die auf dem jeweiligen mobilen Gerät gespeicherten personenbezogenen Daten ebenfalls berichtigt, gesperrt oder gelöscht werden, wenn die betroffene Person ihr Recht auf Berichtigung unrichtiger oder unvollständiger personenbezogener Daten oder ihr Recht auf Sperrung oder Löschung unrechtmäßig verarbeiteter Daten geltend macht.

VI. Risiken für personenbezogene Daten bei der Verarbeitung über mobile Geräte

81 In diesem Abschnitt findet sich eine Liste typischer Risiken und Bedrohungen für personenbezogene Daten auf mobilen Geräten, die die EU-Organe bei der Durchführung ihrer eigenen Risikobewertung berücksichtigen sollten. Die Liste bildet die Grundlage für die Ermittlung der wichtigsten Risiken und Bedrohungen, erhebt jedoch keinen Anspruch auf Vollständigkeit: Die tatsächlichen Risiken und die zur Kontrolle dieser Risiken ergriffenen Sicherheitsmaßnahmen müssen von jedem EU-Organ im Kontext der jeweils durchgeführten Bewertung bestimmt werden.

Als Hilfestellung sind im nachstehenden Schaubild die zentralen Elemente des Risikomanagementprozesses dargestellt.

82 Mobile Geräte bringen mehr Risiken für personenbezogene Daten mit sich als Desktop-Computer aufgrund ihrer Standortunabhängigkeit und, im Fall von Smartphones und Tablets, ihrer Fähigkeit, große Mengen von Kontextinformationen zu erheben und zu übermitteln, ihrer ‚immer online'-Funktion, der Zahl und Vielfalt von Sensoren[17] und der von den Nutzern erwarteten ‚nahtlosen Interaktion'.

83 Die gemischte Nutzung mobiler Geräte zu privaten und dienstlichen Zwecken kann weitere Komplexität mit sich bringen. Im dienstlichen Kontext verarbeitete personenbezogene Daten könnten potenziell unberechtigt verarbeitet werden. Zudem könnte ihre Vertraulichkeit, Integrität und Verfügbarkeit bei der Nutzung zu privaten Zwecken und umgekehrt untergraben werden, auch ohne Wissen des Nutzers.

84 Für personenbezogene Daten bestehen die folgenden zentralen **Risiken**:

- versehentlicher Verlust personenbezogener Daten,
- Änderung oder Vernichtung personenbezogener Daten aufgrund eines unrechtmäßigen Zugriffs auf personenbezogene Daten von Nutzern durch Administratoren mobiler Geräte, einschließlich Fernsperrung, -änderung/-löschung personenbezogener Daten (Fotos, Videos, lokale Kontakte, lokale E-Mail-Kopien, Dokumente usw.),
- Weitergabe personenbezogener Daten aufgrund eines unzulässigen Zugriffs auf diese Daten, der potenziell auch den Ruf oder die Finanzlage des EU-Organs schädigen kann,
- unrechtmäßige geografische Ortung des Nutzers durch potenzielle Angreifer über Standortdienste,
- Identitätsdiebstahl mittels Manipulation von auf mobilen Geräten gespeicherten Nutzerdaten (Benutzernamen, Passwörter, Zertifikate).

85 Folgende zentrale **Bedrohungen** können zu den vorstehend aufgeführten Risiken führen:

- mobile Anwendungen und/oder mobile Geräte, die unrechtmäßig personenbezogene Daten erheben und verarbeiten,

  z. B. geografische Standortdaten der Nutzer ohne ihre Einwilligung, Analyse von Textnachrichten zur Erstellung von Werbeprofilen

- Anpassung durch Gerätehersteller, Netzbetreiber und Betriebssystementwickler, die zu gesperrten Konfigurationen und Funktionen führen,

  wenn beispielsweise Standortsensoren (GPS) nicht deaktiviert werden können oder keine Beschränkung der Daten möglich ist, die das mobile Gerät an den Gerätehersteller oder den Anbieter einer bestimmten Anwendung übermittelt

[17] Zum Beispiel GPS, digitaler Kompass, Gyroskop, Geschwindigkeitsmesser, Umgebungslichtsensor oder Umweltsensoren zur Messung von Luftdruck, Temperatur und Luftfeuchtigkeit.

- mutwillige Nutzung von Sicherheitslücken mobiler Geräte durch Hacker (extern oder intern), um personenbezogene Daten zu manipulieren (direkt oder als Nebeneffekt einer Manipulation geschäftlicher Daten),

> *z. B. eine infizierte pdf-Datei wird an den Nutzer eines mobilen Geräts übermittelt mit dem Ziel, das Gerät derart zu manipulieren, dass die E-Mails des Nutzers gelesen werden können*

- versehentlicher Verlust oder Diebstahl des mobilen Geräts,
- physische Manipulation des Geräts, um Zugang zu auf diesem gespeicherten Daten zu erhalten oder Malware zu installieren,

> *Das mobile Gerät wird unbeaufsichtigt in einem Hotelzimmer oder Besprechungsraum zurückgelassen, sodass ein Dritter auf dem Gerät unbemerkt Anwendungen installieren/modifizieren oder das mobile Gerät physisch verändern kann.*

- Missbrauch,

> *Aufgrund einer fehlerhaften Konfiguration kann der Nutzer die auf dem mobilen Gerät installierte Firewall deaktivieren. Um eine bestimmte Anwendung zu verwenden, deaktiviert der Nutzer die Firewall, obwohl er sich der Tatsache bewusst ist, dass dies gemäß geltenden Bestimmungen untersagt ist.*

- menschliches Versagen.

> *Der Nutzer ignoriert eine Sicherheitswarnung des mobilen Geräts, das in der Folge mit Malware infiziert wird.*

VI.1. Datenschutzverletzungen bei gespeicherten Daten

86 Sind keine geeigneten Maßnahmen zum Schutz der auf mobilen Geräten gespeicherten Daten vor unzulässigem oder unsachgemäßem Zugriff vorhanden, besteht für das EU-Organ die Gefahr potenzieller finanzieller oder physischer Schäden oder von Rufschädigungen.

> *Anhand einiger Beispiele lässt sich diese Gefahr illustrieren:*
> *• Diebstahl eines mobilen Geräts einschließlich der darauf gespeicherten personenbezogenen Daten,*
> *• Entsorgung oder Verkauf eines mobilen Geräts oder Speichermediums ohne vorheriges Löschen personenbezogener Daten, sodass der Finder oder Käufer unter Umständen auf die gespeicherten personenbezogenen Daten zugreifen kann,*
> *• auf dem Gerät gespeicherte organeigene/private Daten können von Anwendungen verwendet werden, die zu privaten/dienstlichen Zwecken genutzt werden,*
> *• Anwendungen für Dateiaustausch und Dateispeicherung können vertrauliche Daten an Dritte übermitteln,*
> *• in der Cloud gespeicherte personenbezogene Daten können manipuliert werden.*

VI.2. Verarbeitung ‚personenbezogener Daten Dritter'

87 Einige der über mobile Geräte verarbeiteten personenbezogenen Daten können sich auf Personen beziehen, die nicht Bedienstete von EU-Organen sind, sog. *personenbezogene Daten Dritter*.

> *Ein Nutzer eines EU-Organs kann beispielsweise Zugang zu einer organeigenen Anwendung haben, die personenbezogene Daten enthält, und diese Daten auf das mobile Gerät herunterladen. Diese neue „Datenbank" („Schattendatenbank") enthält dieselben personenbezogenen Daten wie die „Original"-Anwendung des Organs, ist jedoch nicht über die für letztere eingerichteten Sicherheitsmaßnahmen geschützt (z. B. Zugangskontrolle über strenge Authentifizierungsmechanismen) oder im Falle eines Downloads auf den Arbeitsplatzcomputer des EU-Organs (herkömmliche Hardware).*

88 Wenn man bedenkt, dass bei mobilen Geräten ein höheres Diebstahl- oder Verlustrisiko besteht und die für mobile Geräte umsetzbaren Sicherheitsmaßnahmen beschränkt sind, ist offensichtlich, dass die Datenschutzrisiken bei diesem Szenario wesentlich höher sind als bei einem normalen Zugriff auf die organeigene Datenbank über Arbeitsplatzcomputer.

VI.3. Überwachung der Kommunikation

89 Eine Überwachung der Kommunikation lässt sich definieren als Beobachtung oder Kontrolle der Kommunikation oder Aktivitäten einer Einzelperson. Die Überwachung der Aktivitäten einer Person erfolgt in der Regel auf drei verschiedene Arten: durch Abhören von Kommunikation, durch Auswertung von Daten, die über Kommunikationsaktivitäten erhoben werden (Metadaten), durch Zugriff auf das mobile Gerät selbst.

> *Beispiele für Faktoren und Mittel, die beim Abfangen von Kommunikation zum Einsatz kommen, sind:*
> *• mangelnde Sicherheit von Kommunikationsprotokollen, um E-Mail- und Internetverkehr zu schützen,*
> *• Malware auf Geräten,*
> *• in die Privatsphäre eindringende Anwendungen, die rechtswidrig auf personenbezogene Daten zugreifen und diese verwenden.*
>
> *Ein manipulierter öffentlicher WLAN-Zugangspunkt kann beispielsweise für Man-in-the-Middle-Angriffe verwendet werden, um Kommunikationsdaten der Nutzer abzufangen.*

VI.4. BYOD-spezifische Risiken

90 Die Möglichkeit, dass Bedienstete von EU-Organen ihre eigenen mobilen Geräte nutzen („mitbringen") können, um auf organeigene Daten zuzugreifen, kann Vorteile für die EU-Organe und ihre Bediensteten mit sich bringen. Allerdings ergeben sich auch zusätzliche Risiken. Der Umfang der Kontrollen, die die EU-Organe und ihre IT-Abteilungen ausüben können – auch im Hinblick auf die Gerätekonfiguration,

kann im BYOD-Szenario geringer sein als in einem Szenario, in dem die Geräte und Apps vom EU-Organ im Vorfeld ausgewählt, genehmigt und gemanagt werden.

91 Verbindet sich das mobile Gerät mit dem Netzwerk des EU-Organs, so kann ein zusätzliches Risiko von ihm ausgehen (auch aufgrund der Unmöglichkeit, die Sicherheit des mobilen Geräts zu managen). Schadsoftware und Malware können das mobile Gerät nutzen, um unerlaubten Zugang zu einem gesicherten Netzwerk zu erlangen.

92 Wie bereits erwähnt, vermischen sich im BYOD-Szenario die private und dienstliche Nutzung mobiler Geräte. Für die Organe ergibt sich das Risiko, dass sie unter Umständen Zugang zu personenbezogenen und privaten Daten ihrer Bediensteten erhalten (z. B. durch Zugriff auf mit der organeigenen Infrastruktur synchronisierte personenbezogene Daten). Für die Bediensteten entsteht das Risiko, dass gegebenenfalls organeigene Daten offengelegt werden mittels Nutzung privater Dienste wie Cloud-Speicherung oder -Sicherung (die problemlos vom Nutzer selbst aktiviert werden können) oder über zu privaten Zwecken installierte Anwendungen, die in der Folge als ‚Tor' für den unrechtmäßigen Zugriff auf Daten des EU-Organs missbraucht werden können.

93 Das am Markt verfügbare breite Angebot an mobilen Geräten mit unterschiedlichen Betriebssystemen macht es den IT-Abteilungen der EU-Organe schwierig bis unmöglich, Support für die Auswahl und Verwaltung all dieser Geräte anzubieten. Darüber hinaus wird es der IT-Abteilung kaum möglich sein, Sicherheits-Updates und Konfigurationen zu kontrollieren, die der Nutzer oder Anbieter des mobilen Geräts durchführen und einstellen kann. Nichtsdestotrotz kann die Komplexität und Schwierigkeit – aus rechtlicher und technischer Sicht – der datenschutzrelevanten Aspekte der Datenverarbeitung durch EU-Organe über eine IT-Infrastruktur, in der Bediensteten zur Verfügung gestellte mobile Geräte zum Einsatz kommen, von den EU-Organen nicht als Rechtfertigung einer eventuellen Nichtbeachtung der Bestimmungen der Verordnung herangezogen werden. Und schließlich gilt: Umfasst die Datenverarbeitung eine Verarbeitung besonders sensibler Daten und Informationen, kann das EU-Organ sich gegen die Zulassung der Nutzung mobiler Geräte (organeigen und/oder im Rahmen des BYOD-Szenarios) zur Erhebung, Speicherung und Übermittlung dieser personenbezogenen Daten entscheiden.