Sicherheitsniveau	Erforderliche Elemente
	Art und Weise, wie einschlägige Behörden und Endnutzer informiert werden, sowie Einzelheiten dazu geregelt sein, wie Daten in Übereinstimmung mit den Systemvorgaben zu schützen, aufzubewahren bzw. zu zerstören sind.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.2. Veröffentlichte Bekanntmachungen und Benutzerinformationen

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es gibt eine veröffentlichte Definition des Dienstes mit allen geltenden Geschäftsbedingungen und Entgelten sowie möglichen Nutzungsbeschränkungen. Die Definition des Dienstes enthält auch eine Datenschutzerklärung. 2. Es sind geeignete Vorgaben und Verfahren zu schaffen, damit die Benutzer des Dienstes in rascher und verlässlicher Weise informiert werden, wenn sich die Definition des Dienstes selbst, die geltenden Geschäftsbedingungen oder die Datenschutzerklärung in Bezug auf den betreffenden Dienst ändern. 3. Es sind geeignete Vorgaben und Verfahren zu schaffen, damit Auskunftsersuchen vollständig und richtig beantwortet werden.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.3. Informationssicherheitsmanagement

Sicherheitsniveau	Erforderliche Elemente
Niedrig	Es besteht ein wirksames Informationssicherheitsmanagementsystem für das Management und die Beherrschung von Informationssicherheitsrisiken.
Substanziell	Zusätzlich zum Niveau „Niedrig“: Das Informationssicherheitsmanagementsystem folgt bewährten Normen oder Grundsätzen für das Management und die Beherrschung von Informationssicherheitsrisiken.
Hoch	Wie für das Niveau „Substanziell“.

2.4.4. Aufbewahrungspflichten

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Die Aufzeichnung und Aufbewahrung einschlägiger Informationen erfolgt mit einem effektiven Aufzeichnungsverwaltungssystem unter Beachtung geltender Vorschriften und bewährter Verfahren auf dem Gebiet des Datenschutzes und der Datenspeicherung. 2. Aufzeichnungen werden, soweit nach nationalem Recht oder anderen nationalen Verwaltungsregelungen zulässig, aufbewahrt und geschützt, solange dies für Prüfungszwecke und für die Untersuchung von Sicherheitsverletzungen sowie für die Zwecke der Datenspeicherung erforderlich ist; danach werden die Aufzeichnungen auf sichere Weise vernichtet.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.5. Einrichtungen und Personal

Die folgende Tabelle enthält die Anforderungen an Einrichtungen und Personal sowie an etwaige Unterauftragnehmer, die Aufgaben wahrnehmen, die unter diese Verordnung fallen.

Die Einhaltung jeder dieser Anforderungen soll im Hinblick auf die Risiken des jeweiligen Sicherheitsniveaus verhältnismäßig sein.

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es gibt Verfahren, die sicherstellen, dass alle Mitarbeiter und Unterauftragnehmer eine ausreichende Ausbildung, Qualifikation und Erfahrung bezüglich der ihnen übertragenen Aufgaben haben. 2. Es gibt eine ausreichende Anzahl von Mitarbeitern und Unterauftragnehmern für einen angemessenen Betrieb und eine angemessene Ausstattung des Dienstes entsprechend den Vorgaben und Verfahren. 3. Die zur Bereitstellung des Dienstes genutzten Einrichtungen werden ständig überwacht und vor Schäden durch Umgebungseinflüsse, unbefugten Zugriff oder andere Faktoren geschützt, die die Sicherheit des Dienstes beeinträchtigen können. 4. Die zur Bereitstellung des Dienstes genutzten Einrichtungen gewährleisten, dass nur befugte Mitarbeiter und Unterauftragnehmer Zugang zu Bereichen haben, in denen personenbezogene Daten, kryptografische oder andere sensible Informationen verarbeitet werden.
Substanziell	Wie für das Niveau „Niedrig“.
Hoch	Wie für das Niveau „Niedrig“.

2.4.6. Technische Kontrollen

Sicherheitsniveau	Erforderliche Elemente
Niedrig	1. Es gibt angemessene technische Kontrollen für das Risikomanagement in Bezug auf die Sicherheit der Dienste sowie zum Schutz der Vertraulichkeit, Unversehrtheit und Verfügbarkeit der verarbeiteten Informationen. 2. Elektronische Kommunikationswege, die zur Übermittlung personenbezogener oder sensibler Informationen verwendet werden, müssen gegen Abhören, Manipulation und Replay geschützt sein. 3. Der Zugang zu sensiblem kryptografischen Material, das für die Ausstellung elektronischer Identifizierungsmittel und für die Authentifizierung verwendet wird, ist streng auf die Rollen und Anwendungen beschränkt, die diesen Zugang unbedingt benötigen. Es ist sichergestellt, dass solches Material niemals dauerhaft im Klartext gespeichert wird. 4. Es gibt Verfahren, die gewährleisten, dass die Sicherheit dauerhaft aufrechterhalten wird und dass auf geänderte Risikostufen, Vorfälle und Sicherheitsverletzungen reagiert werden kann. 5. Alle Speichermedien, die personenbezogene, kryptografische oder andere sensible Informationen enthalten, werden in sicherer und geschützter Weise aufbewahrt, transportiert und entsorgt.
Substanziell	Zusätzlich zum Niveau „Niedrig“: Sensibles kryptografisches Material, das für die Ausstellung elektronischer Identifizierungsmittel und für die Authentifizierung verwendet wird, ist vor Fälschung geschützt.
Hoch	Wie für das Niveau „Substanziell“.

2.4.7. Einhaltung und Prüfung

Sicherheitsniveau	Erforderliche Elemente
Niedrig	Es gibt regelmäßige interne Prüfungen (Audits) aller Bestandteile, die für die Bereitstellung der Dienste von Bedeutung sind, um die Einhaltung der betreffenden Vorgaben zu gewährleisten.

ANHANG

Sicherheits-niveau	Erforderliche Elemente
Substanziell	Es gibt regelmäßige unabhängige interne oder externe Prüfungen (Audits) aller Bestandteile, die für die Bereitstellung der Dienste von Bedeutung sind, um die Einhaltung der betreffenden Vorgaben zu gewährleisten.
Hoch	1. Es gibt regelmäßige unabhängige externe Prüfungen (Audits) aller Bestandteile, die für die Bereitstellung der Dienste von Bedeutung sind, um die Einhaltung der betreffenden Vorgaben zu gewährleisten. 2. Wird das System direkt von einer staatlichen Stelle verwaltet, so erfolgen die Prüfungen nach den nationalen Rechtsvorschriften.