

## Fact-Sheet Informationssicherheit im E-Government

Dokument ist ein Auszug aus eCH-0043 sowie aus dem Leitfaden E-Government 2009 des ISB

**Werden Leistungen für Unternehmen und Bürger/innen digitalisiert und im Internet angeboten, stellt sich zwangsläufig umgehend die Frage der Sicherheit. Dieses Fact-Sheet klärt die Begriffe Datenschutz, Integrität und Authentizität, um diese anschliessend in einer Übersicht zur Entscheidungshilfe zusammenzustellen. Am Ende werden kurz die marktgängigen Technologien angeschnitten.**

### 1. Datenschutz oder Persönlichkeitsschutz

Der Persönlichkeitsschutz bezweckt die Wahrung der Persönlichkeitsrechte von natürlichen und juristischen Personen. Informationen können aus Sicht der Datenschutzgesetzgebung keine Relevanz aufweisen, sie können relevant sein (Personendaten) oder sogar eine hohe Persönlichkeitsschutzrelevanz aufweisen (besonders schützenswerte Personendaten und Persönlichkeitsprofile).

#### - keine Persönlichkeitsschutzrelevanz

Keine Persönlichkeitsschutzrelevanz weisen Informationen auf, die keine Angaben zu bestimmten oder bestimmaren juristischen und natürlichen Personen enthalten. Ebenfalls dieser Kategorie werden beispielsweise Informationen zugeordnet, die einzig Name, Vorname und interne Anschrift(en) der Mitarbeitenden der Verwaltung enthalten.

#### - Persönlichkeitsschutzrelevanz

Dieser Klassifizierungsstufe sind Informationen zuzuordnen, die Personendaten enthalten und weder der Schutzstufe *keine Persönlichkeitsschutzrelevanz* noch der Schutzstufe *hohe Persönlichkeitsschutzrelevanz* zugeordnet werden (z.B. AHV-Nummern von Bürgern).

- *hohe Persönlichkeitsschutzrelevanz* Informationen, die besonders schützenswerte Personendaten oder Persönlichkeitsprofile enthalten, sind mit dem Vermerk *hohe Persönlichkeitsschutzrelevanz* zu versehen.

Besonders schützenswerte Personendaten sind Daten über:

- die religiösen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
- die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
- Massnahmen der sozialen Hilfe,
- administrative oder strafrechtliche Verfolgungen und Sanktionen.

Ein Persönlichkeitsprofil ist eine Zusammenstellung von Personendaten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

## 2. Integrität

Informationen unterliegen dann erhöhten Integritätsanforderungen, wenn deren fahrlässige oder absichtliche Veränderung besonders negative Folgen für den Sender oder den Empfänger hätte. Ein Verlust der Integrität bedeutet, dass Daten unberechtigterweise modifiziert werden.

### - normale Integritätsanforderungen

Informationen, deren Integrität nicht durch zusätzlichen technischen Aufwand bei der Übertragung geschützt werden muss.

### - hohe Integritätsanforderungen

Informationen, deren Integrität durch zusätzliche Massnahmen geschützt werden muss (beispielsweise durch das Signieren von E-Mails).

## 3. Authentizität

Der Verlust der Authentizität bedeutet, dass die Identität des Kommunikationspartners gefälscht sein kann, so dass der wahre Ursprung der Informationen nicht sicher eruiert werden kann. Die Authentizität der Kommunikationspartner ist gegeben, wenn eine positive Identifikation beider Parteien stattfindet und so der wahre Ursprung der Daten nachgewiesen werden kann. Die drei Klassifizierungsstufen der Authentizität sind:

### - keine Authentizitätsanforderungen

Die Kommunikationspartner haben keine Authentizitätsanforderungen zu berücksichtigen.

### - Authentizitätsanforderung

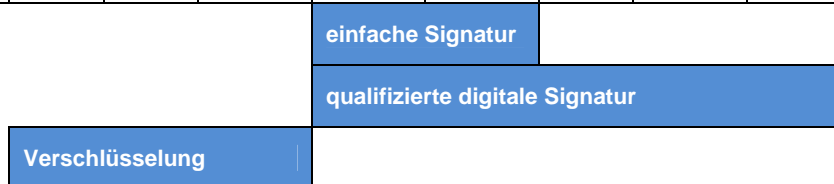
Der Kommunikationspartner soll zum Schutz vor einem Missbrauch der Information im Rahmen der Dienstleistung authentifiziert werden.

### - gesetzliche Authentizitätsanforderung

Der Kommunikationspartner muss aus gesetzlichen Gründen positiv identifiziert werden können.

Entsprechend den gewählten Klassifizierungen werden für die Schutzmassnahmen sowohl Sicherheitstechnologien zur Authentifizierung als auch Technologien zum Schutz der Integrität, des Informationsschutzes und des Persönlichkeitsschutzes benötigt. Um in der Praxis rasch realisierbare Ergebnisse zu erhalten, konzentriert sich die Auswahl der Sicherheitstechnologien auf solche, die bereits eingesetzt werden.

	Datenschutz <i>keine Einsicht</i>			Integrität <i>keine Verfälschung</i>		Authentizität <i>die richtige Person</i>		
	Keine Personendaten	Personendaten	Besonders schützenswerte Personendaten	Normal	Hoch	Nicht erforderlich	Erforderlich	Gesetzlich erforderlich
Web	1	3	5/6	1	2	1	3	5/6
E-Mail	1	6	6	1	2	1	1	6



#	Schutztechnologie-Set
1	Ungeschützt
2	Digital signiert (Eine signierte Übertragung per Web bedeutet den Einsatz von SSL/TLS und Server Zertifikat. Die Web-Sitzung wird gleichzeitig verschlüsselt.)
3	Benutzer-Code mit Passwort und verschlüsselte Verbindung (User-ID/Passwort über SSL/TLS)
4	Benutzer-Code mit Passwort, verschlüsselte Verbindung und Out-of-Band Massnahme (User-ID/Passwort über SSL/TLS und z.B. Code per Briefpost)
5	Benutzer-Code mit Passwort, verschlüsselte Verbindung und One-Time-Password (User-ID/Passwort und One-Time-Password über SSL/TLS oder über VPN mit IPSec, bspw. Einsatz einer SecureID)
6	Digital signiert und verschlüsselt (PKI über SSL/TLS, d.h. Client- und Server Zertifikat, oder VPN mit IPSec)

für Web

#	Schutztechnologie-Set
1	Ungeschützt
2	Digital signiert (E-Mail signiert, aber nicht verschlüsselt)
6	Digital signiert und verschlüsselt (PKI mit S/MIME)

für E-Mail

Hinweis: Das in der Praxis realisierte Schutzniveau wird nicht alleine von der Technologie, sondern insbesondere auch durch deren korrekte Handhabung bestimmt (beispielsweise die Qualität von Registrierungsprozessen).