Amt für Informatik des Kantons Graubünden
Uffizi d'informatica dal chantun Grischun
Ufficio d'informatica del cantone dei Grigioni

7001 Chur, Rosenweg 4 +41 81 257 31 70 info@afi.gr.ch www.afi.gr.ch

Sicherheitsbestimmungen Beschaffung Fachanwendungen

Titel	Sicherheitsbestimmungen Beschaffung Fachanwendungen
Typ	Weisung
Dokument Nr.	AFI-1207
Thema	Informatik-Sicherheit
Version	1.0
Status	Beschlossen
Beschlossen am	30.05.2022
Gestützt auf	Informatik-Verordnung, InfV (BR 170.500), Art. 4, Abs. 2
Beschlossen durch	AFI
In Kraft ab	30.05.2022
Ersetzt	
Inhaltliche Verantwortung	Informatiksicherheitsbeauftragter
Verteiler	
Publikationsort	Verwaltungsverordnungen Internet und AFI-Internet
Klassifizierung	-

Versionsverlauf

Version	Datum	Name	Bemerkungen / Änderungen
1.0	30. Mai 2022	Roman Rüegg	Neuerstellung

Inhalt

1. Allgemeine Bestimmungen

- Die rechtlichen Vorgaben aus dem kantonalen Datenschutzgesetz GR, BR 171.100 sowie dem aktuellen und revidierten Datenschutzgesetz des Bundes, BR 235.1 sowie der entsprechenden Verordnung VDSG werden eingehalten. Das angebotene Produkt/Lösung adressiert die daraus entstehenden Anforderungen zum Datenschutz in den Bereichen Rechtmässigkeit, Transparenz, Verhältnismässigkeit, Zweckbindung, Richtigkeit sowie grenzüberschreitende Bekanntgabe.
- Der Dienstleister informiert bei einem allfälligen Datenschutz- oder Datensicherheitsvorfall unmittelbar die Applikationsverantwortlichen Kontaktperson(en) und den ISB (isb@afi.gr.ch) auf Seiten der kantonalen Verwaltung.
- Ein Konzept zur Sicherstellung des IT-Grundschutzes und der Härtung des Systems/Applikation/Produkts ist vorhanden.
- Aktuelle Sicherheits-Standards werden eingehalten und die top Sicherheitsrisiken sind adressiert. Bei Web-Applikationen gelten diesbezüglich die Risiken gem. OWASP (https://owasp.org/www-project-top-ten/). Dies beinhaltet, nicht abschliessend, folgende Bereiche:
  - die Kodierung/Filterung/Validierung sämtlicher Eingaben und Datenuploads (SQLI, XSS, CSRF)
  - den Einsatz von sicheren, aktuellen und unterstützten Programmbibliotheken
  - sichere Zugriffssteuerung (Benutzer dürfen nicht ausserhalb ihrer Berechtigungen handeln können.)
  - sichere Identifikation und Authentifikation
- Prozesse zum Patch-Management und Vorgehen bei Schwachstellen sind etabliert und vorhanden, insbesondere auch bei Notfallpatches (z. B. Log4J).
- Alle Zugriffe/Authentifizierungen auf das ausgeschriebene Produkt/Lösung aus einem externen Netzwerk sind mittels MFA (2-Faktor Authentifizierung) geschützt oder es sind gleichwertige Schutzfunktionen implementiert (z. B. IP-Restriktionen).
- Beim Einsatz von kryptographischen Verfahren müssen die Vorgaben des BSI (BSI-TR-02102) eingehalten werden (Algorithmen, Protokolle und Schlüssellängen).
- Aktuelle Nachweise der Erfüllung der Sicherheitsvorgaben in Form von Reports aus Verwundbarkeitsscans und/oder manuellen Pentetrationstests sind vorhanden und werden auf Verlangen dem Auftraggeber offengelegt.
- Die kantonale Verwaltung hat ein Audit-Recht zur Überprüfung der vorliegenden Vorgaben und deren Einhaltung.
- Die Daten müssen mittels Backup vollständig und konsistent gesichert werden können (Datenbank, Dokumente, Listen etc.).

2. Besondere Bestimmungen für Cloud-Lösungen

- Die Datenbearbeitung wie auch die temporäre und persistente Ablage aller produktiven Daten, inkl. Backup-Daten, und sämtlicher Transaktionsdaten liegen in der Schweiz und erfolgen unter Anwendung des Schweizer Recht.
- Die Daten in der Cloud müssen bei der Übermittlung (in transit) und bei der Speicherung (at rest) verschlüsselt sein.
- Falls der Speicherort ausserhalb der Schweiz ist, müssen folgende Bedingungen erfüllt sein:
    - Gleichwertiges Datenschutzniveau:
      Falls der Speicherort ausserhalb der Schweiz, jedoch in einem Land mit einem gleichwertigen Datenschutzniveau ist und normal schützenswerte Personendaten ausgelagert werden, müssen die Daten bei der Übermittlung (in transit) und bei der Speicherung (on rest) verschlüsselt sein.
    - Nicht gleichwertiges Datenschutzniveau:
      Falls der Speicherort in einem Land mit einem nicht gleichwertigen Datenschutzniveau (siehe Staatenliste des EDÖB, z. B. die USA) liegt und besonders schützenswerte Personendaten betroffen sind, darf der Schlüssel, zusätzlich zur Verschlüsselung, nur in Besitz der kantonalen Verwaltung sein.
- Das Datacenter, der Applikationsbetreiber und die Entwickler können Zertifizierungen im Bereich Informationssicherheit (z. B. ISO 27001) ausweisen oder alternativ können Nachweise erbracht werden, wie die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung der Informationssicherheit (ISMS) vollzogen wird.