Das Land Steiermark
Tourismus

Förderungsrichtlinie
Security CHECK

Leistungsumfang und Kosten

Mit der vom Tourismusressort gestarteten Initiative „Cyber_Safe“ fördert das Land Steiermark Maßnahmen zur Datensicherung und zum Schutz vor Computerkriminalität. Zugleich werden Hotels, Gastronomiebetriebe sowie Tourismusverbände, Regionalverbände und steiermarkweit agierende touristische Angebotsgruppen bei der Umsetzung der im Mai 2018 in Kraft tretenden Datenschutz-Grundverordnung (DSGVO) unterstützt.
Der im Rahmen des „Cyber_Safe“-Programms geförderte **Security Check** wird durch zertifizierte Experten durchgeführt (Verzeichnis auf www.digitalesteiermark.at).
Der **Security Check** umfasst Beratungsleistungen im Umfang von 12 Stunden, die sowohl geblockt binnen eineinhalb Tagen als auch in mehreren Einheiten über einen längeren Zeitraum erbracht werden können. Mindestens die Hälfte der Beratungsleistung ist vor Ort bzw. im jeweiligen Betrieb oder beim Tourismusverband etc. zu erbringen. Die Kosten für den Security Check sind mit 1.200 Euro exkl. MwSt. pauschaliert.
Die Landesförderung beträgt 50 % des Nettohonorars und ist daher ein Fixbetrag in Höhe von 600 Euro. Die Erbringung unentgeltlicher Mehr- und Zusatzleistungen liegt im Ermessen der jeweiligen Beraterinnen und Berater. Fahrtkosten und Spesen werden nicht gefördert. Die Beauftragung eines zertifizierten Experten durch den Förderungswerber kann erst nach Genehmigung des Förderungsantrags seitens des Tourismusreferats des Landes Steiermark erfolgen.

Inhalte der Beratung und Berichtsform

Zweck des **Security Checks** ist es, die aktuellen Sicherheits-Standards des jeweiligen Betriebs bzw. des Tourismus- oder Regionalverbands oder der touristischen Angebotsgruppe zu dokumentieren, diesen Status zu bewerten und Mängel, Sicherheitslücken und Verbesserungspotenziale aufzuzeigen. Der schriftliche Bericht des beauftragten Experten enthält einen Katalog von empfohlenen Maßnahmen zur Verbesserung des Datenschutzes. Im Zuge der Beratung vor Ort erfolgt auch eine Aufklärung der Datenschutz-Verantwortlichen über die wichtigsten Anforderungen und gesetzlichen Vorgaben der Datenschutz-Grundverordnung (DSGVO).
Die äußere Form und der Umfang des Beratungsberichts zum touristischen **Security Check** liegen im Ermessen der jeweiligen Experten, folgende Aspekte sind dabei zu überprüfen und zu bewerten:

1. **Zugang zur betrieblichen Hardware**
2. **Zugriff auf Daten**
3. **Weitergabe von Daten und Datenzugängen**
4. **Datensicherung**
5. **Organisatorische Datenschutz- und Sicherungsmaßnahmen**

1. Zugang zur betrieblichen Hardware

> Sicherung von Räumen mit betrieblicher EDV-Ausstattung
> Überwachungseinrichtungen (Zutrittssysteme, Videoüberwachung, etc.)
> Festlegungen für Zugangsberechtigungen
> Sicherheitsvorkehrungen bei Reinigungs- und Wartungsarbeiten
> Sicherheitsvorkehrungen bei Telearbeit (Netzwerkzugang von außen)

2. Zugriff auf Daten

> Benutzeridentifikation, Passwortverfahren
> Systeme zur Protokollierung von Zugriffen und deren Kontrolle
> Dokumentation der Eingabeverfahren
> Bildschirmsperren (Passwortschutz bei Arbeitspausen)
> automatische Zugangssperre bei wiederholten Anmelde-Fehlversuchen
> individuelle Benutzerkonten für Mitarbeiter
> Verschlüsselung von Datenträgern
> Berechtigungskonzept und Vergabe von Zugriffsrechten auf Basis des Betriebssystems
> Schutz vor unberechtigten Zugriffen auf IT-Systeme (Firewall, etc.)
> Verwaltung mobiler Datenträger
> Verfahren zur Datenlöschung im Sinne der DSGVO
> Entsorgung von alten Datenträgern, Fehldrucken mit sensiblen Informationen etc.
> Regeln für das Kopieren von Datenträgern
> Umgang mit Mobile Devices (USB-Sticks, externe Festplatten, Tablets, Smartphones)
> Regeln für die Fernwartung von Servern und PCs

3. Weitergabe von Daten und Zugängen

> analoger Datenträger-Transport (Boten, Post etc.)
> elektronischer Datenversand (z.B. Anhänge in E-Mails)
> Auswahl von Auftragnehmern mit Zugriffsberechtigungen im Sinne der DSGVO
> Weitergabe von Zugriffsberechtigungen an Subunternehmen im Sinne der DSGVO
> Schriftliche Regelungen für Auftragnehmer mit Datenzugang im Sinne der DSGVO
> Kontrollmaßnahmen durch Datenschutzkoordinatoren

4. Datensicherung

> Brandschutz- und Wasserschutzmaßnahmen

> unterbrechungsfreie Stromversorgung (USV)

> Aufbewahrung von Sicherungsdatenträgern

> Backup-Verfahren

> Einsatz von Cloud-Lösungen und die damit verbundenen Sicherheitsrisiken

> Virenschutz

> Firewalls

> Notfallplan für externe (oder interne) Angriffe oder bei Schäden durch Feuer, Wasser etc.

5. Organisatorische Datenschutz- und Sicherungsmaßnahmen

> innerbetriebliche Regelungen zur Datensicherheit

> IT-Sicherheitskonzept (Richtlinien, Arbeitsanweisungen etc.)

> Konformität mit der Datenschutz-Grundverordnung

> interne Kontrolle der Datenverarbeitung

> stichprobenartige Überprüfung von Protokollen und Login-Daten (sofern vorhanden)

> Vertretung von mit der EDV befassten Mitarbeitern im Urlaub- und Krankheitsfall

> Absicherung von WLAN Netzwerken (z.B. Gäste WLAN, innerbetriebliches WLAN, etc.)

> Absicherung von elektronischen Zutrittssystemen (z.B. Schlüsselkarten, etc.)