FL1 Offensity
Produktbeschreibung

Verfasser:	Telecom Liechtenstein AG
Datum:	09.02.2021
Version:	V1.2 (ersetzt alle früheren Versionen)
Gültig ab:	09. Februar 2021

FL +423 237 74 00 | www.FL1.li | CH 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6

Inhaltsverzeichnis

FL +423 237 74 00 | www.FL1.li | CH 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6

1. Einleitung

Diese Servicebeschreibung und Nutzungsbedingungen erläutern die Ausprägung aller Anwendungen von FL1 Offensity, die Ihnen als Kunde von Telecom Liechtenstein AG (kurz FL1“) in Zusammenarbeit mit der A1 Digital Deutschland GmbH (kurz „A1 Digital“) angeboten und bereitgestellt werden. Sofern hier nicht Abweichendes geregelt wird, kommen die Allgemeinen Geschäftsbedingungen (AGB Geschäftskunden) von FL1 zur Anwendung: www.fl1.li/agb.

Alle FL1 Offensity Anwendungen sind cloudbasierte Services, die ortsunabhängig genutzt werden können. Die Kunden erhalten die notwendigen Zugangsdaten für die Dauer des gewählten Abonnements.

Kunde für das Service FL1 Offensity kann nur ein Unternehmen sein.

2. Anwendungen

FL1 Offensity hilft Unternehmen dabei, die zur Sicherheit ihrer extern erreichbaren IT-Systeme technische Massnahmen nach dem Stand der Technik ergreifen wollen, laufend Schwachstellen zu erkennen. Eine einheitliche Erfassung aller identifizierten Risiken sowie lösungsorientierte Reports reduzieren die Reaktionszeit des Kunden und ermöglichen eine Dokumentation und Priorisierung der zu setzenden Massnahmen.

FL1 übernimmt keinerlei Verantwortung dafür, dass alle vorhandenen Schwachstellen vollumfänglich erkannt werden. Abhängig von den gewählten Konfigurationen ist es möglich, dass einzelne Systeme oder Schwachstellen übersehen werden.

FL1 Offensity beinhaltet folgende Anwendungen:

- Domain-basiertes Asset Discovery
- Schwachstellen-Scans und Risikobewertung
- „Deep-Web“-Überwachung
- Lösungsorientierte Reports
- Review Gespräche mit Security Experten

2.1. Domain-basiertes Asset Discovery

Auf Basis von Domain-Namen des Kunden (z.B. „example.com“) werden dazugehörende, extern erreichbare IT-Systeme erhoben. Dies umfasst beispielsweise DNS- und Mailserver sowie Subdomains.

2.2. Schwachstellen-Scans und Risikobewertung

Die Systeme werden aus dem Internet netzseitig mit Hilfe von Security-Scannern und automatisierten Analysen untersucht, um Informationen oder Hinweise zu erhalten, die ein Angreifer für die Vorbereitung und Durchführung von virtuellen Einbrüchen nutzen kann. Die eingesetzten Werkzeuge überprüfen aktuell bekannte Schwachstellen von Netzwerkkomponenten, Betriebssystemen, Applikationen und Protokollen, soweit sie aus dem Internet nachweisbar sind. Diese werden im Rahmen einer automatisierten Risikoanalyse bewertet. Der Risikostatus wird dokumentiert und kann jederzeit mit vergangenen Ergebnissen verglichen werden. Bei Bekanntwerden neuer Schwachstellen wird – abhängig von technischer Möglichkeit, Umsetzbarkeit, Risikopotenzial und Relevanz – die Kundeninfrastruktur auf Anfälligkeit überprüft.

FL1 Offensity scannt pro Subdomain maximal eine dahinterliegende IP-Adresse.

FL +423 237 74 00 | www.FL1.li | CH 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6

2.3. „Deep-Web"-Überwachung

Unfreiwillig veröffentlichte Datensätze dritter Plattformen können zu Sicherheitsproblemen führen, da etwa E-Mail-Adressen und Zugangsdaten von den Nutzern dieser Plattformen in fremde Hände geraten. FL1 Offensity überwacht das „Deep Web" (auch „Verstecktes Web"), um veröffentlichte Daten aufzuspüren. Gefundene Datensätze werden auf Basis der Kunden-Domains selektiert und verifiziert, um Kunden über veröffentlichte Datensätze zeitnah zu informieren.

FL1 Offensity gleicht Domains und IP-Adressen der Kunden mit öffentlichen und teilöffentlichen Block- und Blacklisten ab, um eine Servicebeeinträchtigung der Kundendienste möglichst frühzeitig zu erkennen. Einträge auf diesen Listen können auch auf Missbrauch oder Kompromittierung der Kundensysteme hinweisen.

2.4. Lösungsorientierte Reports

Die Ergebnisse der laufenden Scans werden in Form eines schriftlichen Reports über das FL1 Offensity Reporting Dashboard zur Verfügung gestellt. Es wird eine Kategorisierung der ggf. gefundenen Schwachstellen vorgenommen, die Schwachstelle wird beschrieben, ggf. werden weiterführende Informationen und Hinweise zur Behebung der Schwachstelle dargelegt. Der Bericht wird in englischer Sprache verfasst.

Die durch FL1 Offensity erkannten Schwachstellen und Datensätze werden vertraulich behandelt. Auf die Reports kann über die Adresse https://reporting.offensity.com/ zugegriffen werden.

2.5. Review Gespräche mit Security Experten

Bestimmte Schwachstellen sind komplex und eine passende Reaktion darauf kann vielseitig sein. Aus diesem Grund beinhaltet FL1 Offensity Review Gespräche mit einem Security Experten von FL1, welches per Video-call abgehalten wird. Dieser kann Ihnen Sie bei der Interpretation, Priorisierung und Abarbeitung der entdeckten Issues beraten.

3. Nutzungsvoraussetzungen

Für die Nutzung von FL1 Offensity sind unter anderem folgende Voraussetzungen seitens des Kunden zu erfüllen:

- Eine aufrechte Internetverbindung
- Internet Browser (Microsoft Edge, Firefox, Chrome)

3.2. Domain Ownership

Um FL1 Offensity nutzen zu können, muss der Kunde entweder selbst Domain Owner sein, oder die Zustimmung des Domain Owners einholen. Gleichzeitig muss er rechtlich verbindlich garantieren, dass er zur Autorisierung der Security Scans befugt ist.

Die Kunden können bei der Aktivierung der Domain aktuell zwischen den folgenden drei dem „Stand der Technik" entsprechenden technischen Methoden wählen, mit denen FL1 Offensity die Domain-Ownership verifiziert:

- **E-Mail-basierte Domain Control Validation**: Wenn die Bestellung aufgegeben wird, wird eine E-Mail-Adresse aus einer Liste mit akzeptablen Optionen ausgewählt. An diese Adresse wird eine E-Mail gesendet, die einen eindeutigen Validierungscode enthält. Die E-Mail sollte von einer Person empfangen werden, die die Kontrolle über die Domain innehat. Die Liste der zulässigen E-Mail-Adressen für eine bestimmte Domain lautet beispielsweise admin@, administrator@, hostmaster@, postmaster@ oder es handelt sich dabei um eine beliebige E-Mail-Adresse für Administrator, Registrant, Tech oder Zone, die im WHOIS-Verzeichnis aufscheint.

FL +423 237 74 00 | www.FL1.li | CH 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6

- **DNS-based Domain Control Validation**: Der Kunde muss einen vordefinierten Text-code als so genannten DNS-Texteintrag in seine DNS-Verwaltungskonsole hochladen.
- **HTTP-based Domain Control Validation**: Der Kunde muss eine Authentifizierungsdatei in den Stammordner seiner Website hochladen.

3.3. User-Berechtigungen

Für die Bereitstellung von FL1 Offensity benötigen wir Vor- und Zuname, E-Mail-Adresse sowie Mobil-Nummer jener Person/en, auf deren Name/n der Erstzugang und damit die User-Berechtigungen eines Administrators eingerichtet werden sollen.
Administratoren haben folgende User-Berechtigungen:

- Erhalt von Alarmierungen per Email oder SMS
- Aktivierung und Deaktivierung weiterer Domains und Subdomains (inkl. Der dahinterliegenden IP-Adressen)
- Erteilung einer rechtlich verbindlichen Permission to Attack
- Anlegen weiterer Administratoren
- Zugriff auf sämtliche Reports

3.4. Permission to Attack

Die Schwachstellen Scans („Security-Scans“) können „intrusiv“ und „nichtintrusiv“ sein.

- **Intrusive Security-Scans** sind Scans, die technische oder organisatorische Schutzmassnahmen umgehen können. Diese Scans bedürfen einer rechtlich verbindlichen Zustimmung durch den Kunden bzw. einen Administrator, dass die aktivierten Subdomains unter jeder Domain (inkl. den dahinterliegenden IP-Adressen) durch FL1 Offensity auf Schwachstellen gescannt werden dürfen (sog. „Permission to Attack“). Ohne eine solche Zustimmung können diese Scans illegal sein.
- **Nicht-intrusive Security-Scans** sind Scans, die keine technischen oder organisatorischen Schutzmassnahmen umgehen, um auf das Vorhandensein von Schwachstellen zu schliessen. Dies umfasst etwa das Herausfinden von Software-Versionen. Es ist in der Regel keine Zustimmung des System-Besitzers notwendig.

Der Kunde bzw. ein Administrator kann das Hinzufügen von weiteren, bzw. das Löschen von bereits aktivierten Domains und Subdomains über das FL1 Offensity Dashboard durchführen. Diese fallen automatisch unter die davor bereits erteilte domain-basierte Permission to Attack.

Sollte die Permission to Attack zum Zwecke erweiterter Prüfungen über Domains hinaus erweitert werden müssen, kann die Permission to Attack schriftlich durch einen Administrator erteilt werden. Dies könnte beispielsweise bei IP basierten Zielen, internen Netzwerken oder für die Freigabe zu Social Engineering- Kampagnen notwendig sein, etwa im Zuge von erweiterten Leistungspaketen. Eine erteilte Permission to Attack gilt – sofern durch den Kunden schriftlich kommuniziert – in einem festgelegten Zeitrahmen, alternativ bis zum Ende der Vertragslaufzeit oder bis zum Widerruf.

Der Kunde hat dafür zu sorgen, dass jene Systeme, die für Schwachstellen-Scans verwendet werden, von dynamischen Sicherheitseinschränkungen (wie z.B. Web Application Firewalls, fail2ban, etc.) ausgenommen werden. Eine Ausnahme von statischen Sicherheitsmassnahmen (wie etwa Packet Filtering Firewall) ist möglich, wird seitens FL1 aber nicht empfohlen. Die Quellsysteme und deren IP-Adressbereiche, die für Schwachstellen-Scans verwendet werden, werden dem Kunden auf Anfrage mitgeteilt.

3.5. Fair Use Policy

Kommt es während eines Kalendermonats zu einer auffälligen Anzahl an aktivierten Subdomains, so behält FL1 sich das Recht vor zusätzliche Kosten in Rechnung zu stellen.

FL +423 237 74 00 | www.FL1.li | CH 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6

4. Zusatzleistungen

Der Kunde hat die Möglichkeit, kostenpflichtige Zusatzleistungen zu FL1 Offensity zu bestellen. Zusatzleistungen müssen explizit im Vertrag aufgeführt werden, um in Anspruch genommen werden zu können.

4.1. ProSupport

Mit ProSupport hat der Kunde die Möglichkeit, Security-Beratungsgespräche in Bezug auf erbrachte und zukünftig zu erbringenden Leistungen in Anspruch zu nehmen.

Das Gespräch dient zur Besprechung identifizierter Risiken, sowie zur Planung und Abstimmung eventueller zukünftiger Tests. Das Gespräch ist mit einer Vorlaufzeit von zumindest zwei Wochen durch den Kunden aktiv einzufordern. Die Terminfindung geschieht in beiderseitigem Einvernehmen. FL1 empfiehlt die Vereinbarung eines Serientermins.

4.2. Weitere Assessments

FL1 bietet in Zusammenarbeit mit A1 Digital die Möglichkeit an weitere Security Assessments von Systemen und Organisationen durchzuführen.

Der Kunde hat hierbei die Möglichkeit, folgende Assessments zu vereinbaren:

a) Security Assessment extern erreichbarer Systeme, die von FL1 Offensity kontinuierlich gescannt werden und/oder die durch den Kunden explizit mittels Permission to Attack freigegeben wurden.
b) Security-Assessment interner Netzwerkinfrastrukturen des Kunden nach expliziter Freigabe.
c) Individuelle Social Engineering Kampagnen (z.B. Phishing-Kampagnen über E-Mail)

5. Serviceverfügbarkeit

Hinweis: In diesem Service sind keine technischen Unterstützungsleistungen enthalten.

- Nutzungszeit: Montag bis Freitag, 09:00-17:00 Uhr.
  Die Nutzungszeit ist der Zeitraum, in dem die grundsätzliche Leistung dem Kunden zur Nutzung zur Verfügung steht.
- Beobachtungszeitraum: ein Kalenderjahr
- Verfügbarkeit FL1 Offensity: 96%

  Die Verfügbarkeit ist das in Prozent ausgedrückte Verhältnis zwischen der Zeit, in der eine vereinbarte Leistung vertragskonform nutzbar war, und dem Beobachtungszeitraum. Ausschliesslich kritische Fehler sind verfügbarkeitsrelevant.

  $$Verfügbarkeit\ [\%] = \frac{(Beobachtungszeitraum - nicht\ verfügbare\ Zeit)}{Beobachtungszeitraum} * 100$$

- Wartungsfenster: Die regelmässige Wartung von FL1 Offensity Services kann eine geplante Serviceunterbrechung erforderlich machen. Daher werden Unterbrechungen, die zur Wartung des Service erforderlich sind, für einen im Voraus definierten Zeitraum, dem so genannten Wartungsfenster, von FL1 Offensity geplant. Darüber hinaus können ausserordentliche Wartungsarbeiten durchgeführt werden, die ausserhalb des Wartungsfensters betriebsnotwendig sind.
- Fremdverzögerungen können zu einer nicht von FL1 zu verantwortenden Verlängerung der Wartungsarbeiten führen.
- Das Wartungsfenster ist üblicherweise am Mittwoch 14:00 – 18:00 Uhr.

FL +423 237 74 00 | www.FL1.li | CH 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6

6. Haftungsausschluss

FL1 weist darauf hin, dass die Durchführung von Security-Scans und Penetrationstests die Verfügbarkeit und Integrität der Zielsysteme beeinträchtigen kann. Es ist möglich, dass der ordnungsgemässe Betrieb nur durch manuellen Zugriff auf das Zielsystem wiederhergestellt werden kann. Dies bedeutet beispielsweise, dass die Webseite auf dem Zielsystem nicht mehr erreichbar sein könnte, bzw. dass Registrierungen, Anmeldungen oder Bestellungen mit unrichtigen Daten durchgeführt werden könnten. Der Kunde hat allein für alle hierdurch eingetretenen nachteiligen Folgen einzustehen.

Jede identifizierte Subdomain muss durch den Kunden explizit freigeschalten werden, damit sie gescannt wird. Mit dem Freischalten der Subdomain gibt der Kunde verbindlich bekannt, dass er die Befugnis hat, dahinterliegende IP-Adressen attackieren zu lassen. Bei Änderung der DNS-Einträge auf weitere oder andere IP-Adressen ist der Kunde dazu verpflichtet, die Subdomain zu deaktivieren. Bei Nicht Deaktivierung darf FL1 Offensity davon ausgehen, dass der Kunde die Befugnis hat, auch die aktualisierten IP-Adressen zu attackieren.

Alle Fragen betreffend Rechte an den Domains (z.B. Registrierung, Innehabung, Sperre, Kauf, Miete, Pacht, Sharing, Urheberrechte, Namensrecht, Markenrecht und allenfalls daraus resultierende Konflikte wird der Kunde im eigenen Bereich abschliessend lösen.

FL1 leistet gegenüber dem Kunden Schadenersatz oder Ersatz vergeblicher Aufwendungen, gleich aus welchem Rechtsgrund (z.B. aus rechtsgeschäftlichen und rechtsgeschäftsähnlichen Schuldverhältnissen, Pflichtverletzung und unerlaubter Handlung), in folgendem Umfang:

a) Die Haftung bei grober Fahrlässigkeit, Vorsatz, Arglist und aus Garantie wird hierdurch nicht vertraglich eingeschränkt.

   Auch für Schäden aus der schuldhaften Verletzung des Lebens, des Körpers oder der Gesundheit und bei Ansprüchen nach dem Produkthaftungsgesetz gelten die gesetzlichen Regelungen uneingeschränkt.

b) Bei Verletzung einer vertragswesentlichen Pflicht, deren Erfüllung also die ordnungsgemässe Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmässig vertrauen darf (sog. Kardinalpflicht), haftet FL1 nur in Höhe des bei Vertragsabschluss typischerweise vorhersehbaren Schadens.
c) Die Haftung für einfache Fahrlässigkeit ist gegenüber dem Kunden (und auch Körperschaften des öffentlichen Rechts) bei Verletzung einer nicht vertragswesentlichen Pflicht ausgeschlossen.
d) Soweit die Haftung von FL1 nach dem Vorstehenden ausgeschlossen oder beschränkt ist, gilt dies auch für die persönliche Haftung der Mitarbeiter, Vertreter und Erfüllungsgehilfen von FL1.
e) Für Schäden, die aus einer vertragswidrigen Verwendung der Leistungen von FL1 Offensity resultieren, haftet FL1 nicht.

7. Kontakte

Kommerzielle Fragen und Bestellungen:	Sales, Telecom Liechtenstein AG, E-Mail: sales@telecom.li
Technische Fragen und Störungen:	Tel. +423 237 90 90, security@telecom.li

FL +423 237 74 00 | www.FL1.li | CH 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6

8. Kündigung, Mindestvertragsdauer

Die Mindestvertragsdauer für FL1 Offensity beträgt 6 Monate. Die Mindestvertragsdauer wird ab Datum der Aktivierung berechnet. Nach Ablauf der Mindestvertragsdauer ist der Vertrag unbefristet und kann mit einer Kündigungsfrist von 30 Tage per Ende Monat aufgelöst werden. Allfällige Zusatzpakete setzen eine Mindestvertragsdauer von 1 Monat voraus.

Nach erfolgter Kündigung eines Abonnements besteht kein Zugriff mehr auf die Instanz.

9. Datenschutz

FL1 fungiert als qualifizierter Reselling-Partner für Offensity. Durch den Kauf von FL1 Offensity akzeptieren Sie die Nutzungsbedingungen des Herstellers für diesen Dienst. Es gelten die Bestimmungen entsprechend dem A1 Digital Endkunden-Nutzungsvertrag, die in geltender Fassung auf der offiziellen Website des Herstellers zu finden sind.

A1 Digital setzt grösste Anforderungen an den Schutz Ihrer Daten und an die Zufriedenheit mit deren Produkten. Im Rahmen des Kaufes der Produkte akzeptieren Sie die folgenden Lizenzbestimmungen hinsichtlich Nutzungsrechten, Sicherheit und Datenschutz:

- ✓ Offensity Security Monitoring & Reporting - Servicebedingungen
- ✓ Offensity Security Monitoring & Reporting - Servicebeschreibung
- ✓ Allgemeinen Geschäftsbedingungen der A1 Digital für IoT und Security Solutions
- ✓ Allgemeine Geschäftsbedingungen der A1 Digital International GmbH für Auftragsverarbeitung (AGB AVV)
- ✓ Datenschutzerklärung der A1 Digital

Diese sind in der jeweils gültigen Fassung unter „https://www.a1.digital/at/ueber-a1-digital/agbs“ abrufbar.

FL1 gibt für die Erbringung des Service ausschliesslich notwendige Informationen an A1 Digital Deutschland GmbH weiter. Weitere Informationen zu den Datenschutzbestimmungen von FL1 können unter www.fl1.li/datenschutz entnommen werden.

9.1. Datenschutzanhang zur Leistungsbeschreibung

In Rahmen der von FL1 bereitgestellten Leistungen werden personenbezogenen Daten im Sinne der Datenschutzrichtlinie von FL1 behandelt.

a) Liste der beauftragten Subunternehmer

Name	Firmenadresse	Art der Verarbeitung	Ort der Verarbeitung
A1 Digital Deutschland GmbH	St. Martin-Strasse 59, 81669 München, Deutschland	Applikationsbetreuung und Auswertung	Deutschland, Österreich

b) Technisch-organisatorische Massnahmen

FL1 stellt die Sicherheit in punkto Datenschutz und Datensicherheit, die in der Datenschutzrichtlinie von FL1 geregelt ist, her. Insgesamt handelt es sich bei den zu treffenden Massnahmen um Massnahmen zur Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher

FL +423 237 74 00 | www.FL1.li | CH 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6

Personen zu berücksichtigen. Sofern in der Leistungsvereinbarung nicht genauer geregelt, obliegt es FL1, das der jeweiligen Verarbeitung angemessene Schutzniveau insbesondere durch eine Kombination der nachstehend genannten technisch-organisatorischen Massnahmen sicherzustellen. Es ist dem FL1 gestattet, alternative adäquate Massnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Massnahmen nicht unterschritten werden.

A. VERTRAULICHKEIT

- **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B. durch Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung durch z.B.(sichere) Kennwörter, Zwei-Faktor-Authentifizierung.
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch, z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.
- **Trennungskontrolle:** Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. durch Standard-Berechtigungsprofile auf „need to know-Basis“, Mandantenfähigkeit.
- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.
- **Klassifikationsschema für Daten:** Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

B. DATENINTEGRITÄT[1]

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch z.B. Verschlüsselung.
- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch z.B. Protokollierung.

C. VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch z.B. Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Firewall, Meldewege und Notfallpläne.
- **Wiederherstellbarkeit**

D. VERFAHREN ZUR REGELMÄSSIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- **Datenschutz-Management, einschliesslich regelmässiger Mitarbeiter-Schulungen**
- **Incident-Response-Management**
- **Datenschutzfreundliche Voreinstellungen**
- **Auftragskontrolle:** Keine Auftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers.

[1] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

FL +423 237 74 00 | www.FL1.li | CH 0800 423 000 | www.FL1.ch
Telecom Liechtenstein AG | Schaanerstrasse 1 | LI-9490 Vaduz | FL1@telecom.li | MWST-Nr. 53836 | HReg. Liechtenstein | Reg.Nr. FL-0001.545.008-6