Sicherheitsvorkehrungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

Dieses Dokument enthält eine allgemeine Beschreibung der organisatorischen und technischen Sicherheitsvorkehrungen von POST bei der Verarbeitung personenbezogener Daten im Rahmen der Erfüllung von Verträgen mit ihren Geschäftskunden.

EINLEITUNG

POST ergreift geeignete technische und organisatorische Maßnahmen, um ein angemessenes Sicherheitsniveau für personenbezogene Daten zu gewährleisten, die von POST im Namen des Kunden verarbeitet werden. Die von POST getroffenen Sicherheitsvorkehrungen zielen darauf ab, personenbezogene Daten vor Sicherheitsverletzungen zu schützen, die unbeabsichtigt oder unrechtmäßig zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung personenbezogener Daten oder zum unbefugten Zugriff auf diese Daten führen. Das implementierte Sicherheitsniveau hängt von der jeweiligen Verarbeitung personenbezogener Daten ab, wobei Art, Umfang, Kontext und Zwecke der Verarbeitung, die Art der verarbeiteten Daten sowie die festgestellten Risiken für die Rechte und Freiheiten der betroffenen Personen berücksichtigt werden. Dieses Sicherheitsniveau berücksichtigt auch den Wissensstand und die Kosten der Umsetzung.

1. Maßnahmen zur Pseudonymisierung und Verschlüsselung personenbezogener Daten

POST ist als der für die Datenverarbeitung Verantwortliche und/oder als Auftragsverarbeiter um die Pseudonymisierung und/oder Verschlüsselung personenbezogener Daten unter Anwendung möglicher Techniken für verschiedene Szenarien bemüht. Jeder Fall einer Verarbeitung personenbezogener Daten muss vor dem Hintergrund der damit verbundenen Risiken analysiert werden, um die am besten geeignete technische Option in Bezug auf die Pseudonymisierung und Verschlüsselung personenbezogener Daten zu bestimmen.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	POST hat Richtlinien für Datenverschlüsselung und Key-Management erarbeitet, in denen die Anforderungen für die Anwendung der Verschlüsselung und den Schutz der kryptografischen Schlüssel festgelegt sind.
2	Erstellung und Validierung eines vertrauenswürdigen signierten Zertifikats zur Verschlüsselung sensibler Daten und zur Sicherung des HTTPS-basierten Webzugangs
3	Gegebenenfalls werden sichere Authentifizierungsprotokolle verwendet (FTPS, LDAPS, SSH usw.).
4	Standardmäßig werden Produktivdaten mit echten personenbezogenen Daten nicht in der Test- und Entwicklungsumgebung verwendet.
5	Pseudonymisierungstechniken werden durch Trennung der Daten von direkten Identifikationsmerkmalen umgesetzt, um zu verhindern, dass ohne zusätzliche Informationen eine Verbindung zu der betroffenen Person hergestellt wird.
6	Die Festplattenvollverschlüsselung ist auf den Systemlaufwerken der Arbeitsstationen aktiviert.
7	Die Verwendung von Produktivdaten, die personenbezogene Daten oder vertrauliche (C3) oder streng vertrauliche (C4) Daten enthalten, ist nur unter den folgenden Bedingungen zulässig: • C3- und/oder C4-Produktionsdaten werden gemäß ISO/IEC 29101 gelöscht oder geändert oder • die technischen und organisatorischen Sicherheitsvorkehrungen sind identisch mit denen in der Produktivumgebung.

	Das Kopieren von Produktivdaten in eine Testumgebung erfordert die vorherige Freigabe durch den Eigentümer der Anwendung. Diese Anträge müssen zu Prüfzwecken dokumentiert werden.
	Vgl. ISO 27001:2013 – A.15 Cryptography / A.12 Operations security

2. Maßnahmen zur ständigen Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten

POST ist als der für die Datenverarbeitung Verantwortliche und/oder als Auftragsverarbeiter um die Einführung technischer und organisatorischer Kontrollmechanismen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Datenverarbeitungssysteme und -dienste bemüht.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Die Datenbank und die Anwendungen sind so konfiguriert, dass sie für eine korrekte Funktionsweise unter einem separaten Account mit minimalen Betriebssystemrechten ausgeführt werden.
2	Datenbank- und Anwendungsserver verarbeiten nur die personenbezogenen Daten, deren Verarbeitung für die Verarbeitungszwecke tatsächlich erforderlich ist.
3	Für bestimmte Dateien oder Aufzeichnungen werden Verschlüsselungslösungen durch Software- oder Hardware-Implementierung in Betracht gezogen.
4	Gegebenenfalls werden Speicherlaufwerke mit Verschlüsselung verwendet.
5	Mitarbeiter, die mit der mit hohen Risiken behafteten Verarbeitung personenbezogener Daten befasst sind, sind an besondere Vertraulichkeitsklauseln gebunden (gemäß Arbeitsvertrag oder einem anderen Rechtsakt).
6	POST stellt sicher, dass alle Mitarbeiter ihre Aufgaben und Pflichten im Zusammenhang mit der Verarbeitung personenbezogener Daten kennen. Rollen und Zuständigkeiten werden während des Pre-Employment- und/oder Einarbeitungsprozesses klar kommuniziert.
7	Vor Aufnahme ihrer Tätigkeit werden die Mitarbeiter aufgefordert, die Sicherheitsrichtlinien des Unternehmens zu lesen und zu akzeptieren und entsprechende Vertraulichkeits- und Geheimhaltungsvereinbarungen zu unterzeichnen.
8	POST hat die wichtigsten einzuhaltenden Kontrollen zur Gewährleistung des erforderlichen Maßes an Kontinuität und Verfügbarkeit des IT-Systems für die Verarbeitung personenbezogener Daten (im Fall eines Vorfalls/einer Verletzung des Schutzes personenbezogener Daten) festgelegt.
	Vgl. ISO 27001:2013 – A.12 Operations security / A.15 Supplier relationships / A.7 Human resource security / A.17 Information security aspects of business continuity management

3. Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit und den Zugriff auf personenbezogene Daten im Falle eines physischen oder technischen Vorfalls zügig wiederherzustellen

POST implementiert ein Backup-System für die Wiederherstellung bei Verlust oder Vernichtung von personenbezogenen Daten. Die Häufigkeit und die Art der Sicherung hängen von der Art der verarbeiteten Daten ab. POST erfüllt Art. 32 DSGVO in Bezug auf den Aspekt der „Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen" als Teil der Datensicherheitsverpflichtungen für den Verantwortlichen oder den Auftragsverarbeiter.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Backup- und Datenwiederherstellungsverfahren sind definiert, dokumentiert und klar mit Rollen und Verantwortlichkeiten verknüpft.

POST Luxembourg
Adresse postale : POST Luxembourg L-2020 Luxembourg / Tél. +352 2424-1 / Fax +352 47 51 10 / contact.group@post.lu
Siège : 20, rue de Reims L-2417 Luxembourg / RCS Luxembourg : J28 / TVA : LU 15400030
www.postgroup.lu

Maßnahmen-Nr.	Beschreibung der Maßnahme
2	Die Backups werden entsprechend den für die Ursprungsdaten geltenden Standards in angemessenem Umfang physisch und umgebungsseitig geschützt.
3	Die Durchführung von Backups wird überwacht, um deren Vollständigkeit zu gewährleisten.
4	Es werden regelmäßig vollständige Backups durchgeführt.
5	Die Backup-Medien werden regelmäßig getestet, um sicherzustellen, dass sie im Notfall verlässlich sind.
6	Geplante inkrementelle Backups werden mindestens einmal am Tag durchgeführt.
7	Kopien des Backups werden an verschiedenen Orten sicher aufbewahrt.
8	Kopien von Backups werden verschlüsselt und auch sicher offline aufbewahrt.
	Vgl. ISO 27001:2013 – A.12.3 Back-Up

Im Falle einer Verletzung des Schutzes personenbezogener Daten prüft POST, ob diese „ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden" (Art. 4(12) DSGVO). POST stellt sicher, dass die Pflichten gemäß Art. 33 und 34 DSGVO bezüglich der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und die betroffenen Personen erfüllt werden. POST stellt auch sicher, dass sie ihrer Pflicht gemäß Art. 33 DSGVO zur unverzüglichen Meldung als Verantwortlicher nachkommt. In jedem Fall hat POST geeignete Verfahren eingerichtet, nicht nur für die Meldung von Verletzungen des Schutzes personenbezogener Daten, sondern auch für den allgemeinen Umgang mit solchen Ereignissen.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Richtlinien und Pläne mit detaillierten Verfahrensabläufen zur Reaktion auf Vorfälle wurden erarbeitet, um eine wirksame und geordnete Reaktion auf Vorfälle im Zusammenhang mit personenbezogenen Daten zu gewährleisten.
2	Verletzungen des Schutzes personenbezogener Daten werden unverzüglich an die Geschäftsleitung gemeldet. Meldeverfahren für die Meldung von Sicherheitsverletzungen an die zuständigen Behörden und die betroffenen Personen gemäß Art. 33 und 34 DSGVO sind eingerichtet.
3	Der Plan für die Reaktion auf Vorfälle ist dokumentiert, einschließlich einer Liste möglicher Abhilfemaßnahmen und einer klaren Rollenzuweisung.
4	Vorfälle und Verletzungen des Schutzes personenbezogener Daten werden zusammen mit den Einzelheiten des Ereignisses und den daraufhin ergriffenen Abhilfemaßnahmen aufgezeichnet.
	Vgl. ISO 27001:2013 – A.16 Information security incident management

4. Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Technisch setzt POST dies durch eine Reihe von technischen Maßnahmen wie Schwachstellen-Scans, Penetrationstests sowie regelmäßige Sicherheitsbewertungen und interne/externe Audits für kritische Systeme und Infrastrukturen um. Diese Maßnahmen dienen im Wesentlichen dazu, potenzielle Risikobereiche und verbesserungswürdige Aspekte aufzudecken.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Während der Entwicklung werden Tests und Validierungen durchgeführt, um sicherzustellen, dass die ursprünglichen Sicherheitsanforderungen erfüllt sind.

POST Luxembourg
Adresse postale : POST Luxembourg L-2020 Luxembourg / Tél. +352 2424-1 / Fax +352 47 51 10 / contact.group@post.lu
Siège : 20, rue de Reims L-2417 Luxembourg / RCS Luxembourg : J28 / TVA : LU 15400030
www.postgroup.lu

Maßnahmen-Nr.	Beschreibung der Maßnahme
2	Falls erforderlich, werden im Anschluss an die Sicherheitsbewertung durch CyberForce und vor der operativen Umsetzung Schwachstellenanalysen sowie Penetrationstests für Anwendungen und Infrastrukturen durchgeführt. Die Anwendung wird erst dann eingeführt, wenn das erforderliche Sicherheitsniveau erreicht ist.
3	Software-Patches sollten getestet und bewertet werden, bevor sie in einer operativen Umgebung installiert werden.
4	Das Zugangskontrollsystem sollte in der Lage sein, die Verwendung von Passwörtern zu erkennen und zu unterbinden, die nicht einem bestimmten (konfigurierbaren) und in den Sicherheitsrichtlinien von POST festgelegten Komplexitätsgrad entsprechen.
5	Die Sicherheitsanforderungen sind im PPMO (POST Portfolio Management Office) enthalten, d. h. im Prozess „Eingebaute Sicherheit/Datenschutz" und in den Dokumentationen, die auf Ebene der POST-Gruppe definiert sind. Bei jedem neuen Projekt sind die Sicherheitsschritte für die Validierung zu befolgen.
6	Auf der Grundlage der Informationssicherheitsrichtlinien von POST wurden unter anderem folgende Verfahren eingeführt: • Schwachstellen- und Patch-Management-Prozess • Konfigurationsmanagement-Prozess • Protokollierungs- und Überwachungsprozess • Prozess des logischen Zugriffsmanagements KPI und KRI dieser Prozesse werden der Geschäftsleitung regelmäßig gemeldet.
	Vgl. ISO 27001:2013 – A.12.6 Technical vulnerability management / A.14.2 Security in development and support processes

POST Luxembourg
Adresse postale : POST Luxembourg L-2020 Luxembourg / Tél. +352 2424-1 / Fax +352 47 51 10 / contact.group@post.lu
Siège : 20, rue de Reims L-2417 Luxembourg / RCS Luxembourg : J28 / TVA : LU 15400030
www.postgroup.lu

5. Maßnahmen zur Identifizierung und Autorisierung der Benutzer

POST setzt die Zugriffskontrolle und Authentifizierung als grundlegende Sicherheitsmaßnahmen zum Schutz vor unbefugtem Zugriff auf das für die Verarbeitung personenbezogener Daten verwendete IT-System ein.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Jeder Rolle (die an der Verarbeitung personenbezogener Daten beteiligt ist) werden spezifische Zugriffskontrollrechte nach dem Need-to-Know-Prinzip (RBAC-Modell – rollenbasierte Zugriffskontrolle) zugewiesen.
2	Für alle Benutzer, die auf das IT-System zugreifen. ist ein IAM-System (Identitäts- und Zugriffsmanagement) implementiert. Das System ermöglicht das Anlegen, Genehmigen, Überprüfen und Löschen von Benutzerkonten.
3	Die Verwendung generischer/gemeinsamer Benutzerkonten ist standardmäßig untersagt.
4	Ein Authentifizierungsmechanismus, der den Zugang zum IT-System ermöglicht (auf der Grundlage der Richtlinien und des Systems für die Zugriffskontrolle), ist vorhanden. Mindestvorgabe ist eine Kombination aus Benutzername und Passwort. Passwörter müssen einen bestimmten (konfigurierbaren) Komplexitätsgrad gemäß den Sicherheitsrichtlinien der POST-Gruppe aufweisen.
5	Das Zugriffskontrollsystem ist in der Lage, Passwörter zu erkennen und zu unterbinden, die nicht einen bestimmten (konfigurierbaren) Komplexitätsgrad aufweisen.
6	Spezifische dokumentierte Passwortrichtlinien wurden festgelegt. Die Richtlinien enthalten Vorgaben für die Länge, Komplexität und Gültigkeitsdauer von Passwörtern sowie die Anzahl der zulässigen Fehlversuche bei der Anmeldung.
7	Die Trennung der Zugriffskontrollrollen (z. B. Zugriffsanforderung, Zugriffsberechtigung, Zugriffsverwaltung) ist klar definiert und dokumentiert.
8	Für alle Remote-Zugriffe auf das Netzwerk von POST wird die Zwei-Faktor-Authentifizierung angewendet. Zu den Authentifizierungsfaktoren gehören Passwörter und ein Einmalpasswort.
9	Mit der Geräteauthentifizierung wird gewährleistet, dass die Verarbeitung personenbezogener Daten nur über bestimmte Ressourcen im Netzwerk erfolgt.
10	Rollen mit umfassenden Zugriffsrechte sind klar definiert und nur bestimmten Mitarbeitern zugewiesen.
11	Der Zugriff auf das IT-System erfolgt nur über vorher autorisierte Geräte und Endgeräte.
	Vgl. ISO 27001:2013 – A.9 Access control / A.9.1.1 Access control policy

6. Maßnahmen zum Schutz der Daten bei der Übermittlung

POST implementiert Netzwerksicherheitsmaßnahmen zum Schutz personenbezogener Daten sowohl für externe Verbindungen (z. B. zum Internet) als auch für Verbindungen zu anderen (externen oder internen) Systemen des Unternehmens.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Erfolgt der Zugriff über das Internet, wird die Kommunikation durch kryptografische Protokolle (TLS/SSL) verschlüsselt.
2	Der Wireless-Zugang zum IT-System ist durch Verschlüsselungsmechanismen geschützt.
3	Der Datenverkehr zum und vom IT-System wird durch Firewalls und IDS (Intrusion Detection Systems) überwacht und gesteuert.
4	Das Netzwerk des Informationssystems ist von den anderen Netzen des Verantwortlichen getrennt.
	Vgl. ISO 27001:2013 – A.13 Communications Security / A. 14.1 Security requirements of information systems

POST Luxembourg
Adresse postale : POST Luxembourg L-2020 Luxembourg / Tél. +352 2424-1 / Fax +352 47 51 10 / contact.group@post.lu
Siège : 20, rue de Reims L-2417 Luxembourg / RCS Luxembourg : J28 / TVA : LU 15400030
www.postgroup.lu

7. Maßnahmen zum Schutz der Daten während der Speicherung

POST wendet Sicherheitsrichtlinien zum Schutz der Daten während der Speicherung an. Das bedeutet unter anderem, dass Benutzer bestimmte Aktionen nicht ausführen können, die die Sicherheit des IT-Systems gefährden könnten (z. B. Deaktivierung von Virenschutzprogrammen oder Installation nicht autorisierter Software).

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Die Benutzer haben keine Möglichkeit, die Sicherheitseinstellungen zu deaktivieren oder zu umgehen.
2	Virenschutzanwendungen und Erkennungssignaturen werden täglich konfiguriert.
3	Die Benutzer haben keine Berechtigungen zur Installation nicht autorisierter Softwareanwendungen oder zur Deaktivierung installierter Software.
4	Im System sind Sitzungs-Timeouts eingerichtet, sodass ein Benutzer automatisch abgemeldet wird, wenn er eine bestimmte Zeit lang nicht aktiv war.
5	Kritische Sicherheitsupdates werden regelmäßig gemäß den Sicherheitsrichtlinien der POST-Gruppe installiert.
6	Die Festplattenvollverschlüsselung ist auf den Systemlaufwerken der Arbeitsstationen aktiviert.
	Vgl. ISO 27001:2013 - A. 14.1 Security requirements of information systems

8. Maßnahmen zur Gewährleistung der physischen Sicherheit der Orte, an denen personenbezogene Daten verarbeitet werden

POST ergreift physische Sicherheitsmaßnahmen für Büroräume und das Rechenzentrum, wo personenbezogene Daten verarbeitet werden.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	POST hat Richtlinien für die physische Sicherheit erarbeitet und einen PSO (Physical Security Officer) ernannt.
2	Der physische Zugang wird protokolliert. Der PSO nimmt regelmäßige Überprüfungen des physischen Zugangs und Kontrollen der physischen Sicherheit vor.
3	Für Gebäude und das Rechenzentrum werden Videoüberwachungssysteme eingesetzt.
4	Bereiche mit eingeschränktem Zugang werden regelmäßig überprüft/kontrolliert.
5	Interne und/oder externe Audits der physischen Sicherheitsvorkehrungen für die Räumlichkeiten und das Rechenzentrum von POST werden jährlich im Rahmen der ISO27001-Zertifizierung durchgeführt.
6	Für alle Mitarbeiter und Besucher, die die Räumlichkeiten des Unternehmens betreten, wird ggf. eine eindeutige Identifizierung durch das Tragen eines Ausweises implementiert.
7	Durch entsprechende Zugangskontrollen geschützte Sicherheitszonen sind vorhanden. Ein physisches Protokollbuch oder ein elektronischer Audit-Trail wird für alle Zugriffe sicher geführt und überwacht.
8	In allen Sicherheitsbereichen sind Einbruchmeldesysteme installiert.
9	Gegebenenfalls werden physische Barrieren errichtet, um unbefugten physischen Zugang zu verhindern.
10	Leerstehende Sicherheitsbereiche werden physisch verschlossen und regelmäßig kontrolliert.
11	In den Serverräumen sind ein automatisches Feuerlöschsystem, ein geschlossenes Klimatisierungssystem und eine unterbrechungsfreie Stromversorgung (USV) installiert.
12	Externes Supportservicepersonal erhält eingeschränkten Zugang zu Sicherheitsbereichen.

POST Luxembourg
Adresse postale : POST Luxembourg L-2020 Luxembourg / Tél. +352 2424-1 / Fax +352 47 51 10 / contact.group@post.lu
Siège : 20, rue de Reims L-2417 Luxembourg / RCS Luxembourg : J28 / TVA : LU 15400030
www.postgroup.lu

Maßnahmen-Nr.	Beschreibung der Maßnahme
	Vgl. ISO 27001:2013 – A.11 - Physical and environmental security

9. Maßnahmen zur Sicherstellung der Ereignisprotokollierung

Die Verwendung von Protokolldateien ist eine wesentliche Sicherheitsmaßnahme, die die Identifizierung und Verfolgung von Benutzeraktionen (bei der Verarbeitung personenbezogener Daten) ermöglicht und somit die Rechenschaftspflicht im Falle einer unbefugten Offenlegung, Änderung oder Vernichtung personenbezogener Daten unterstützt. Die Überwachung der Protokolldateien ist wichtig, um mögliche interne oder externe Versuche einer Systemverletzung zu erkennen.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Für jedes System/jede Anwendung, das/die für die Verarbeitung personenbezogener Daten verwendet wird, werden automatisch Protokolldateien erstellt. Diese sollten alle Arten des Datenzugriffs umfassen (Ansicht, Änderung, Löschung).
2	Die Protokolldateien werden mit einem Zeitstempel versehen und in geeigneter Weise vor Manipulationen und unbefugtem Zugriff geschützt. Die Uhren werden über eine zentrale Referenzuhr synchronisiert.
3	Aktionen der Systemadministratoren und Systembetreiber, z. B. das Hinzufügen, Löschen oder Ändern von Benutzerrechten, werden protokolliert.
4	Es besteht keine Möglichkeit, den Inhalt der Protokolldateien zu löschen oder zu ändern. Der Zugriff auf die Protokolldateien sollte zusätzlich zur Überwachung auf ungewöhnliche Aktivitäten protokolliert werden.
5	Ein Überwachungssystem sollte die Protokolldateien verarbeiten und Berichte über den Status des Systems erstellen und bei Bedarf Warnmeldungen ausgeben.
	Vgl. ISO 27001:2013 – A.12.4 Logging and monitoring

10. Maßnahmen zur Sicherstellung der Systemkonfiguration, einschließlich der Standardkonfiguration

Sichere Konfiguration bezieht sich auf Sicherheitsmaßnahmen, die bei der Installation und Einrichtung von Computern und Netzwerkgeräten umgesetzt werden, um unnötige Cyberschwachstellen zu minimieren und Sicherheitsrisiken zu vermeiden.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	POST hat einen Leitfaden für die Konfiguration der Systemhärtung erstellt.
2	POST hat ein Konfigurationsmanagementverfahren eingeführt, um sichere Systemkonfigurationen zu gewährleisten.
3	Die Konfigurationen kritischer IT-Systeme werden regelmäßig überprüft, um sicherzustellen, dass sie den grundlegenden Anforderungen, Standards und bewährten Verfahren entsprechen.
	Vgl. ISO 27001:2013 – A.12 Operations Security

POST Luxembourg
Adresse postale : POST Luxembourg L-2020 Luxembourg / Tél. +352 2424-1 / Fax +352 47 51 10 / contact.group@post.lu
Siège : 20, rue de Reims L-2417 Luxembourg / RCS Luxembourg : J28 / TVA : LU 15400030
www.postgroup.lu

11. Maßnahmen für interne IT- und IT-Sicherheits-Governance und -Management

a. Richtlinien für die Informationssicherheit

POST hat ein ISMS (Information Security Management System) eingerichtet, das die Informationssicherheitsrichtlinien sowie spezifische Richtlinien für bestimmte Bereiche umfasst. Einige verwandte Prozesse sind auch im Framework aufgeführt, um die Einhaltung der Kontrollanforderungen von ISO27001:2013 zu belegen.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Die Informationssicherheitsrichtlinien und spezifischen Richtlinien werden den Mitarbeitern und relevanten Dritten auf Need-to-Know-Basis mitgeteilt.
2	Alle Informationssicherheitsrichtlinien von POST werden regelmäßig überprüft und aktualisiert.
	Vgl. ISO 27001:2013 – A.5 Information security policies

b. Organisation der Informationssicherheit

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Die Rollen und Zuständigkeiten im Bereich der Informationssicherheit sind in den Informationssicherheitsrichtlinien festgelegt.
2	Der Compliance-Beauftragte von POST ist der Ansprechpartner für die zuständigen Behörden in Sicherheitsbelangen. Der Datenschutzbeauftragte von POST ist der Ansprechpartner für die Datenschutzbehörde.
3	Der Kontakt zu besonderen Interessengruppen wird von verschiedenen Funktionen bei POST gepflegt, z. B. dem Compliance-Beauftragten, dem Beauftragten für Informationssicherheit, dem Datenschutzbeauftragten usw.
4	Ein Verfahren zur Bewertung der Informationssicherheit („Security by Design") für neue Projekte und neue Produkte für das Management der Sicherheitsrisiken wurde eingeführt.
5	Ein Verfahren für eingebauten Datenschutz (Privacy by design), das auf neue Projekte und Produkte angewendet wird, ist eingerichtet. Zu diesen Prozessen gehören Risikobewertung, Penetrationstests und Datenschutz-Folgeabschätzungen.
6	POST hat Risikomanagementrichtlinien und -verfahren für das Management von Betriebs- und Sicherheitsrisiken eingeführt. Bewertungen der operativen und Sicherheitsrisiken, insbesondere für kritische IT-Systeme/Umgebungen, werden regelmäßig durchgeführt.
	Vgl. ISO 27001:2013 – A.6 Organization of information security

c. Sicherheit im Personalmanagement

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	POST hat für alle Unternehmen von POST Onboarding- und Offboarding-Prozesse für Überprüfungen im Vorfeld von Personaleinstellungen eingeführt.
2	Neue Mitarbeiter werden hinreichend überprüft und einer Hintergrundprüfung unterzogen.
3	Neue Mitarbeiter erhalten ein Willkommenspaket mit folgendem Inhalt: • Informationssicherheitsrichtlinien • „Sécurité de l'information et la protection des données personnelles" (Booklet) • Merkblatt zu den spezifischen Sicherheitsanforderungen von POST Telecom (aufgrund ihres Status als unterstützender Finanzdienstleister und ihrer ISO27001-Zertifizierung)
4	Die Geschäftsleitung verlangt von den Mitarbeitern und Subunternehmern von POST, dass sie die festgelegten Richtlinien und Verfahren beachten.

POST Luxembourg
Adresse postale : POST Luxembourg L-2020 Luxembourg / Tél. +352 2424-1 / Fax +352 47 51 10 / contact.group@post.lu
Siège : 20, rue de Reims L-2417 Luxembourg / RCS Luxembourg : J28 / TVA : LU 15400030
www.postgroup.lu

Maßnahmen-Nr.	Beschreibung der Maßnahme
5	Kontrollen, ob die Richtlinien und Verfahren beachtet werden, erfolgen auf unterschiedliche Weise, z. B. durch jährliche Clean Desk & Clean Screen Checks, die Überprüfung der KPIs für Sicherheitsvorfälle usw.
6	POST führt jährliche Schulungen und Veranstaltungen zur Sensibilisierung für Sicherheitsbelange für alle ihre Unternehmen, einschließlich POST Telecom, durch. Jährlich werden Phishing-Kampagnen durchgeführt, um die Reaktion der Mitarbeiter zu testen.
	Vgl. ISO 27001:2013 – A.7 Human Resource security

12. Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

POST Telecom ist nach ISO 27001:2013 für ihr Informationssicherheitsmanagementsystem (ISMS) zertifiziert. Dies belegt den hohen Reifegrad der Management- und Betriebsprozesse ihrer Infrastruktur für die Bereitstellung von Managed Services (lokal oder in der Cloud) sowie aller Support-Prozesse für die Bereitstellung dieser Dienste für ihre Kunden. Die ISO27001-Zertifizierung belegt die Expertise von POST Telecom in diesem Bereich und bietet den Kunden ein hohes Maß an Sicherheit für ihre Managed Services sowie hohe Garantien für die Standardisierung der Managementprozesse von POST Telecom.

13. Maßnahmen zur Gewährleistung der Einhaltung der Datenschutzgrundsätze

Die Achtung der Rechte von Kunden, Mitarbeitern und Partnern ist Teil der Werte von POST. In dieser Hinsicht ist POST bestrebt, personenbezogene Daten innerhalb des strengen Rahmens der Vorschriften und im Einklang mit ihrem Bestreben nach Transparenz, Ethik und Achtung der Privatsphäre zu verarbeiten. POST hat verschiedene Ziele für die Verarbeitung personenbezogener Daten festgelegt.

POST verpflichtet sich in ihren Datenschutzrichtlinien, nur personenbezogene Daten zu verarbeiten, die angemessen und relevant sind und für die Erreichung der vorgegebenen Zwecke unbedingt verarbeitet werden müssen.

a. Privacy by Design/Default

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	POST hat „Privacy by Design"-Richtlinien für alle neuen Produkte oder Verarbeitungstätigkeiten eingeführt, bei denen sie personenbezogene Daten in ihrer Funktion als Auftragsverarbeiter verarbeitet, um sicherzustellen, dass die Prozesse und Systeme so gestaltet sind, dass die Erhebung und Verarbeitung (einschließlich Verwendung, Weitergabe, Aufbewahrung, Übermittlung und Vernichtung) darauf beschränkt sind, was für die festgelegten Zwecke des Verantwortlichen angemessen, relevant und notwendig ist.
2	POST hat globale Richtlinien für die Speicherung personenbezogener Daten eingeführt, um sicherzustellen, dass die Aufbewahrungsfristen für die Daten auf den für die Erreichung ihrer eigenen relevanten Datenverarbeitungstätigkeiten unbedingt erforderlichen Zeitraum begrenzt bleiben. Die Aufbewahrungsfristen werden mit Beginn der Projektphase festgelegt und richten sich nach den Zwecken und Kategorien der verarbeiteten personenbezogenen Daten.
3	Mechanismen zur Berichtigung personenbezogener Daten und zu ihrer Unkenntlichmachung, wenn sie nicht mehr benötigt werden, werden mit der Beginn der Projektphase berücksichtigt.
4	Temporäre Dateien, die infolge der Verarbeitung personenbezogener Daten generiert werden, werden nach dokumentierten Verfahren innerhalb eines bestimmten, dokumentierten Zeitraums gelöscht oder vernichtet.

POST Luxembourg
Adresse postale : POST Luxembourg L-2020 Luxembourg / Tél. +352 2424-1 / Fax +352 47 51 10 / contact.group@post.lu
Siège : 20, rue de Reims L-2417 Luxembourg / RCS Luxembourg : J28 / TVA : LU 15400030
www.postgroup.lu

Maßnahmen-Nr.	Beschreibung der Maßnahme
5	Personenbezogene Daten werden über angemessen geschützte Datenübertragungsnetze übertragen, damit die Daten ihren Bestimmungsort erreichen.
	Vgl. ISO 27701:2019 – 7.4 Privacy by design and privacy by default / 8.4 Privacy by design and privacy by default

b. Pflichten gegenüber Verantwortlichen

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	POST hat Mechanismen zur rechtzeitigen Erkennung von Datenschutzverletzungen eingerichtet.
2	POST hat ein operatives Verfahren eingeführt, mit dem sichergestellt wird, dass (potenzielle) Datenschutzverletzungen so schnell wie möglich an ihre Geschäftskunden gemeldet werden.
3	POST hat operative Verfahren eingeführt, um ihre Geschäftskunden bei der Erfüllung ihrer Pflichten als Verantwortliche zu unterstützen: • Durchführung von Datenschutz-Folgenabschätzungen (DPIA) und • Unterstützung bei der Bearbeitung von Anträgen von betroffenen Personen
4	Nach Ende des Vertrags werden die personenbezogenen Daten an den Kunden zurückgegeben und/oder auf sichere Weise vernichtet.
	Vgl. ISO 27701:2019 – 8.3 Obligations to PII principals

c. Rechenschaftspflicht

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	POST verfügt über ein Datenschutzmanagementsystem (DPMS), um die Erfüllung der Rechenschaftspflicht für die Verarbeitung personenbezogener Daten und deren Kontrolle zu gewährleisten.
2	POST hat die Verarbeitungstätigkeiten, die im Namen ihrer Geschäftskunden durchgeführt werden, dokumentiert. Dazu gehören: - Kategorien der Verarbeitungsvorgänge, die im Namen der einzelnen Kunden durchgeführt werden - Übertragungen in Drittländer oder an internationale Organisationen und - eine allgemeine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen
3	POST hat die Liste der Länder und internationalen Organisationen dokumentiert, an die personenbezogene Daten unter Umständen übermittelt werden.
	Vgl. ISO 27701:2019 – 8.2.6 Records related to processing PII / 8.5 PII sharing, transfer, and disclosure

14. Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung von Daten

POST hat Richtlinien und Maßnahmen festgelegt, um die personenbezogenen Daten unwiderruflich zu löschen oder zu vernichten, sodass sie nicht wiederhergestellt werden können. Die angewendete/n Methode/n ist/sind auf die Art der Speichertechnologie abgestimmt, einschließlich Kopien in Papierform. Bei der Vernichtung veralteter oder redundanter Geräte stellt POST sicher, dass alle zuvor auf den Geräten gespeicherten Daten vor der Vernichtung gelöscht wurden.

POST Luxembourg
Adresse postale : POST Luxembourg L-2020 Luxembourg / Tél. +352 2424-1 / Fax +352 47 51 10 / contact.group@post.lu
Siège : 20, rue de Reims L-2417 Luxembourg / RCS Luxembourg : J28 / TVA : LU 15400030
www.postgroup.lu

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	Alle Datenträger werden vor ihrer Entsorgung softwarebasiert überschrieben (sicheres Format gemäß den Richtlinien von POST). In Fällen, in denen dies nicht möglich ist (CDs, DVDs usw.), erfolgt eine physische Vernichtung.
2	Das für die Speicherung personenbezogener Daten verwendete Papier ist zu vernichten.
3	Werden die Dienste eines Dritten für die sichere Entsorgung von Datenträgern oder Aufzeichnungen in Papierform in Anspruch genommen, wird eine Dienstleistungsvereinbarung geschlossen und ggf. muss eine Bestätigung über die Vernichtung vorgelegt werden.
4	Nach der softwarebasierten Löschung sollten zusätzliche hardwarebasierte Maßnahmen wie die Entmagnetisierung durchgeführt werden. Im Einzelfall kann auch eine physische Vernichtung in Betracht gezogen werden.
	Vgl. ISO 27001:2013 – A. 8.3.2 Disposal of media / A. 11.2.7 Secure disposal or re-use of equipment

15. Bei Übermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter ergreifen muss, um den Verantwortlichen zu unterstützen.

Maßnahmen-Nr.	Beschreibung der Maßnahme
1	POST hat Richtlinien für das Lieferantenmanagement für das Management ihrer Lieferanten und externen Berater eingeführt.
2	Alle Subunternehmer haben Vertraulichkeitsvereinbarungen unterzeichnet, in denen ihre Verantwortung für den Schutz aller Informationen von POST (z. B. personenbezogene Daten, Infrastrukturen usw.) festgelegt ist.
3	Subunternehmer nehmen jährlich an einer Schulung zur Sensibilisierung für Sicherheitsbelange teil.
4	Die Sicherheitsanforderungen an die ausgelagerten Dienstleistungen wurden in dem Vertrag zwischen POST und ihren Lieferanten festgelegt. Regelmäßig finden Besprechungen zur Überprüfung der Lieferanten statt, um die ausgelagerten Dienstleistungen, einschließlich der Sicherheitsaspekte, zu managen.
	Vgl. ISO 27001:2013 – A.15: Supplier Relationships

POST Luxembourg
Adresse postale : POST Luxembourg L-2020 Luxembourg / Tél. +352 2424-1 / Fax +352 47 51 10 / contact.group@post.lu
Siège : 20, rue de Reims L-2417 Luxembourg / RCS Luxembourg : J28 / TVA : LU 15400030
www.postgroup.lu