Technische und organisatorische Maßnahmen

Datum	05.11.2021
Version	1.2
Vertraulichkeit	öffentlich

LogPay Financial Services GmbH
Schwalbacher Straße 72 | DE 65760 Eschborn | www.logpay.de

Inhaltsverzeichnis

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle

Maßnahmen, um Unbefugten den Zutritt zu Räumlichkeiten zu verwehren, in denen personenbezogene Daten verarbeitet werden:

- Die Räume verfügen über ein Schließsystem mit Sicherheitsschlössern.
- Ein Zutritt ohne Befugnis ist nicht möglich.
- Der Zutritt von Besuchern ist nur in Begleitung durch Mitarbeiter zulässig.
- Schächte (Klimaanlage, Umluftanlage, Aufzug usw.) gesichert
- Schlüsselregelung
- Schließregelung (Türen und Fenster sind immer geschlossen zu halten, Alarmanlage im Objekt bei Abwesenheit immer scharf geschaltet)
- Kennzeichnung der Notausgänge und Fluchtwege
- Zutrittsregelungen für Personen und Personengruppen (Mitarbeiter, Führungskräfte, Firmenfremde, Besucher, Wartungs-, Reinigungspersonal, Lieferanten, Boten usw.)
- Regelung beim Ausscheiden und Wechseln von Berechtigten
- Regelungen/Folgemaßnahmen bei Verlust von Ausweisen, Schlüsseln usw.
- Besucherregelung
- Anmeldung und Begleitung von Besuchern und Firmenfremden
- Revisionsfähige Vergabe und Entzug der Zutrittsberechtigungen
- Kontrolle des Wartungs-, Reparatur- und Reinigungspersonals
- Kontrolle von Besuchern

1.2 Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Es erfolgt eine Begrenzung der Zugangsberechtigten.
- Den Benutzern werden Benutzerrechte in Abhängigkeit von den von ihnen ausgeübten Funktionen zugewiesen.
- Eine Authentifizierung erfolgt mit Benutzernamen und Passwort.
- Es existieren Vorgaben zur Passwortgestaltung, -handhabung und -verwaltung.
- Es wird auf allen PCs Antivirensoftware mit automatisierter Aktualisierung eingesetzt.
- Regelungen für die Vergabe und Verwaltung von Zugangsberechtigungen
- Regelmäßige Kontrolle der Gültigkeit der Zugangsberechtigungen
- Zugangsberechtigte weisen sich durch personenbezogene Benutzerkennung und Passwort aus Verwaltung der Passwörter von Notfallbenutzern (Administrator, root usw.)
- Regelung der Verwendung von Passwörtern durch eine Passwort-Policy
- Regelung für Sperrung des Arbeitsplatzrechners beim Verlassen
- Regelung beim Ausscheiden und Wechseln von Berechtigten
- Regelungen bei Verlust oder Vergessen des Passwortes/Passwörter
- Begrenzung der Anmeldeversuche
- Trennen der Verbindung bei wiederholten Fehlversuchen oder Zeitüberschreitungen
- Getrennte Netzwerke für Büro, Services und Gäste
- Einsatz von Firewalls und Virenscanner
- Einsatz von Intrusion Prevention Systemen (IPS) und Absicherung gegen·DDoS Angriffe
- Regelmäßige Kontrolle der Konfigurationen und Abgleich dieser gegen die Vorgaben zur Härtung von Systemen
- Festlegung der Personen, die zur Anmeldung von außerhalb befugt sind
- Netzzugangssicherungen durch Hard- und Softwaremaßnahmen - z.B. ausschließlich VPN- Zugänge mit 2-Faktor-Anmeldung
- Regelung für den Fernzugang von Geschäftspartnern (Extranet)

- Verhinderung des unberechtigten Zugriffs aus dem Internet (Firewall)
- Nachweis der Benutzung von DV-Systemen (Protokollierung der Zugänge)
- Protokollierung der fehlgeschlagenen Zugangsversuche
- Protokollierung der Vergabe/Änderung von Zugangsberechtigungen

1.3 Zugriffskontrolle

Maßnahmen, um zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Die Zugriffsberechtigungen werden in Abhängigkeit von der Funktion eines Mitarbeiters vergeben.
- Die Anzahl der Administratoren ist begrenzt.
- Der Zugriff auf Anwendungen wird protokolliert.
- Für die Vernichtung papiergebundener personenbezogener Daten stehen Aktenvernichter zur Verfügung(Silberne Tonne).
- Regelungen für die Vergabe und Verwaltung von Zugriffsberechtigungen
- Servicebezogene Definition der Regelung der Befugnisverwaltung für Eingabe, Kenntnisnahme, Veränderung und Löschung gespeicherter Daten (Detaillierungsgrad, Vergabepraxis, Unterschriftsberechtigung)
- Individuelle Zugriffsrechte - Bildung von Benutzergruppen
- Richtlinien für die Dateihaltung (z. B. Verfallsdatum, Aufbewahrungsfristen, Schutzklassen)
- Passwortschutz bei Dateien
- Trennung von Test- und Produktionsbetrieb
- Netzzugriffssicherungen
- Einschränkung der Erlaubnis zur Anwendung von Hilfsprogrammen bzw. Funktionen, die geeignet sind, Sicherheitsmaßnahmen zu umgehen
- Zonen durch Zutrittskontrollsystem abgesichert
- Regelung über gesicherte Datenträgeraufbewahrung in Abhängigkeit von der Art der Datenträger (unbeschrieben/neu, beschrieben etc.)
- Organisatorische Regelungen zur Datenträgeraufbewahrung (Aufbewahrungsfristen, eindeutige Kennzeichnung von Datenträgern)
- Festlegung der zur Datenträgerentnahme befugten Personen (Schlüsselverwaltung/Quittierung, Rückgabe)
- Keine Reparatur von Datenträgern, sondern grundsätzlich Entsorgung mit Bestätigung der datenrechtlichen Vernichtung und Entsorgungsnachweis
- Regelung der Anfertigung/Ausgabe von Kopien und Duplikaten (Archivbestände innerhalb und außerhalb des Betriebs, Druckergebnisse usw.)
- Regelung der Vernichtung von Datenträgern in Abhängigkeit von der Art der Datenträger (HDD, Magnetbänder, Flashspeicher, Disketten usw.)
- Protokollierung der Vergabe/Änderung von Zugriffsberechtigungen

1.4 Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung von personenbezogenen Daten, die zu unterschiedlichen Zwecken erhoben wurden:

- Die Verarbeitung von Daten verschiedener Auftraggeber erfolgt getrennt.
- Logische Trennung der Daten
- Mandantenfähigkeit von Anwendungen
- Berechtigungskonzept berücksichtigt die Vergabe von Rechten für unterschiedliche Zwecke
- Trennung von Systemen für Produktion, Test und Entwicklung
- Restriktiver Einsatz von SQL
- Innerbetriebliche Vorgaben für die Datenerhebung und -verarbeitung
- Dokumentation der Datenbank(en)
- Dokumentation der Verarbeitungsprogramme
- Dokumentation der Datenerhebungszwecke

1.5 Verschlüsselung

Maßnahmen zur Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können:

- Einsatz von Verschlüsselungsroutinen (Datenträger- bzw. Dateiverschlüsselung) gemäß der Risikoklassifizierung
- Verschlüsselung von Passwörtern
- Verschlüsselte Übertragung von Daten aus bzw. nach externen Netzen mittels geeigneter Transportprotokolle (SSL/TLS, SSH, S/MIME, PGP usw.

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt verarbeitet werden können:

- Der Zugriff auf personenbezogene Datensätze des Auftraggebers erfolgt nach Möglichkeit und nach Maßgabe der vertraglichen Vereinbarung über verschlüsselte Zugänge (https bzw. SSH).
- Die Weitergabe von Daten ist nur nach Maßgabe der vertraglichen Vereinbarungen und auf Weisung des Auftraggebers zulässig.
- Es werden Logprotokolle erzeugt.
- Die Abfrage und Übertragung personenbezogener Daten durch Anwender erfolgt verschlüsselt mittels Webbrowser (HTTPS). Passwörter der Nutzer werden in der Datenbank nach Möglichkeit verschlüsselt abgelegt.
- Verschlüsselte Übertragung von Daten aus bzw. nach externen Netzen mittels geeigneter Transportprotokolle (SSL/TLS, SSH, S/MIME, PGP usw.)
- Festlegung der Stellen (Dritte), an die durch Einrichtungen der Datenübertragung Daten übermittelt werden können
- Festlegung der Personen, die zur Übermittlung befugt sind (Berechtigungskonzept)
- Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege
- Dokumentation der Abruf- und Übermittlungsprogramme (z. B. FTP, Firewall, Remote Access)
- Protokollierung der Datenübermittlung und der Empfänger
- Eine Speicherung von personenbezogenen Daten auf Wechseldatenträgern ist nicht vorgesehen
- Transport von Datenträgern mit personenbezogenen Daten ist nicht vorgesehen

2.2 Eingabekontrolle

Maßnahmen, um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme verarbeitet worden sind:

- Es gibt ein Protokoll der Eingaben, Veränderungen oder Löschungen personenbezogener Daten.
- Es werden serverseitige Logprotokolle über Nutzerzugriffe geführt.
- Es besteht ein Berechtigungskonzept.
- Die Protokollierung erfolgt im Rahmen der Funktionen in den vom Auftraggeber beauftragten Anwendungsprogramme.
- Regelungen für die Umsetzung eines 4-Augen-Prinzips
- Differenzierte Benutzerrollen (z. B. lesen, schreiben, ändern/löschen)

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Datensicherung: Es erfolgt eine tägliche Sicherung der Daten. Die Daten werden nach erfolgter Sicherung auf getrennten Servern abgelegt.
- Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO): Die Wiederherstellung der Daten aus den Backups kann jederzeit beauftragt werden. Die Wiederherstellbarkeit wird exemplarisch bzw. nach gesonderter Beauftragung durch den Auftraggeber geprüft.
- Generelles Datensicherungskonzept
- Regelmäßige Sicherung der Benutzerdateien, Datenbanken
- Namenskonventionen für Sicherungsdateien (TDS)
- Kennzeichnung der Datenträger (TDS)
- Verwendung des Schreibschutzes bei Datenträgern (TDS)
- Bestandsverzeichnis der Sicherungskopien (Dateien, Datenträger) (TDS)
- Archivordnung (TDS)
- Bestandskontrolle von Datenträgern (TDS)
- Protokollierung von Sicherheitsspeicherungen (TDS)
- Lagerung von Kopien an besonders geschützten Orten
- Festlegung von Aufbewahrungsfristen
- Stromversorgung:
  - Unterbrechungsfreie Stromversorgung durch zwei USV Anlagen für das Rechenzentrum
  - USV für das NOC mit ausreichender Kapazität (USV Überbrückung bis zu 1 Stunde)
  - Regelmäßige Tests der Notstromversorgung (Last- und Leerlauftests)
  - Wartungsverträge vorhanden
- Brandschutz:
  - Aufschaltung auf die Haus BMZ zur Weiterleitung an die Berufsfeuerwehr
  - Zusätzlich Aufschaltung auf die Alarmanlage bei Auslösung (Gasflussmesser im Rohrsystem) mit Weiterleitung auf die ständig besetzte Stelle des Wachdienstes
  - Benachrichtigung der verantwortlichen Mitarbeiter des AUFTRAGNEHMERS durch den Wachdienst bei Auslösung
  - Mehrmals täglich Überprüfung des Tableaus der BMZ des AUFTRAGNEHMERS
  - Wartungsvertrag vorhanden
- Klimatisierung: (TDS)
  - Wartungsvertrag vorhanden
- IP-Anbindung:
  - Redundante Internetanbindung mit getrennter Wegeführung und getrennter Hauseinführung
- Telefonie-Anbindung des Backbone:
  - Das Backbone ist an mindestens zwei Carrier angebunden
- Notfallplan bei Katastrophen (inkl. Zuständigkeiten, Wiederanlaufkonzept, Rufbereitschaften, Ausweichmöglichkeit für Rechenzentrum usw.)
- Business-Continuity-Policy
- Disaster-Recovery-Policy
- Regelmäßige Tests von Bestandteilen der Konzepte
- Funktionstrennung zwischen Fachabteilung und DV-Abteilung
- Zentrale und einheitliche Beschaffung von Hard- und Software
- Formalisierte Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in Altverfahren
- Nur Einsatz geprüfter Fremdsoftware
- Vorgaben für Verfahrens- und Programmdokumentationen
- Erlass von Dienstanweisungen und Sicherheitsrichtlinien

- Angemessene Schulung der Anwender
- Bestellung eines Sicherheitsbeauftragten

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO)

Die in dieser Anlage beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen werden mindestens einmal jährlich geprüft und bei Bedarf angepasst. Bei Feststellung eines sicherheitsrelevanten Vorfalls werden die getroffenen Maßnahmen umgehend geprüft und im erforderlichen Umfang angepasst.

4.1 Auftragskontrolle

Maßnahmen, um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Die Auswahl von Auftragsverarbeitern erfolgt sorgfältig unter Beachtung der Bestimmung des Art. 28 DSGVO.
- Weisungen an die beauftragten Auftragsverarbeiter erfolgen mindestens in Textform.
- Der Auftragnehmer hat einen fachkundigen Datenschutzbeauftragten benannt.
- Die Mitarbeiter des Auftragnehmers werden schriftlich auf den vertraulichen Umgang mit personenbezogenen Daten verpflichtet.
- Die Mitarbeiter des Auftragnehmers werden regelmäßig über die Verpflichtungen unterrichtet, welche sich aus der Auftragsverarbeitung ergeben.
- Sämtliche personenbezogenen Daten werden nach Beendigung des Auftrags bzw. nach Ablauf gesetzlicher Aufbewahrungsfristen gelöscht.
- Wenn beim Auftragnehmer eine Prüfung durch die Aufsichtsbehörde stattgefunden hat, so kann der Auftraggeber den Prüfbericht verlangen. Gleiches gilt für Prüfungen bei möglichen Unterauftragnehmern.
- Betrieb eines Informationssicherheit Management Systems (ISMS)
- Regelungen für den Umgang mit Datenschutz- und Sicherheitsvorfällen
- Regelungen für Anfragen von Betroffenen