Aufstellung gem. Art. 32 DSGVO der opta data Österreich GmbH Linz

- zu den bei der opta data Österreich GmbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz –

Diese Auflistung der bei der opta data Österreich GmbH getroffenen technischen und organisatorischen Maßnahmen orientiert sich an Art. 32 DSGVO und soll es ermöglichen, dem Auftraggeber seine Prüf- und Dokumentationspflicht bei Auftragsverarbeitung gem. Art. 28 und 29 DSGVO zu erleichtern. Die Bestimmungen des DSG 2018 wurden berücksichtigt. Eine strukturierte, übersichtliche und transparente Dokumentation der technischen und organisatorischen Maßnahmen ist gewährleistet.

Diese Aufstellung ist auch als Ergänzung zu einem bestehenden oder neuen, Art. 28 und 29 DSGVO konformen, Auftragsverarbeitungsvertrag gedacht und kann jedem Auftraggeber/ Verantwortlichen auf Anforderung zur Verfügung gestellt werden.

Ergänzend sei noch erwähnt, dass die opta data Österreich GmbH Linz ein „Tochterunternehmen" der opta data finance GmbH (od FIN) in Essen ist. Die Betreuung der Abrechnungssoftware sowie der IT erfolgt durch die od FIN, die die Software auch entwickelt hat. Die IT der od FIN ist nach DIN/ISO 27001 zertifiziert.

I. Allgemeiner Teil

1. Name und Anschrift des Unternehmens

opta data Österreich GmbH
Salzburger Straße 205
A-4030 Linz

2. Kontakt

-Verwaltung-
Tel.: +43 (0)732 38 08 38 -0
Fax: +43 (0)732 38 08 38 -21
E-Mail: office@optadata.at

3. Name der Geschäftsführer

Rainer Strassl, Geschäftsführer
Sylvia Brandstätter, Prokuristin

4. Datenschutzbeauftragter

4.1 Name und Kontaktdaten der Datenschutzbeauftragten:

Sylvia Kramer
Datenschutz Kramer & Kramer GmbH
Richard-Wagner-Str. 11b
D-01445 Radebeul
Tel.: +49 (0)351 833 87 15
Fax: +49 (0)351 833 87 16

4.2 Bestellung:

- externe Datenschutzbeauftragte gem. Art. 37 DSGVO
- schriftliche Bestellung vom 01.01.2013 liegt vor

4.3 Qualifikation:
externe Datenschutzbeauftragte gem. Art. 37 DSGVO

Datenschutz-Auditorin (TÜV) Zertifizierungsstelle für Personal TAR-ZERT der TÜV-Akademie Rheinland, Nr. 19553Datenverarbeitungskauffrau, Grundkurs zum Erwerb von Fachkunde im Sinne des § 4f BDSG der Bundesrepublik Deutschland bei der TÜV-Akademie Berlin, Seminar „Ein Jahr novelliertes BDSG" bei der Gesellschaft für Datenschutz und Datensicherung e. V., Bonn, IT-Grundlagenkurs bei der TÜV-Akademie Rheinland GmbH in Köln, Seminar zur Datenschutzmanagerin TÜV-Akademie Rheinland GmbH in Bad Kreuznach, Seminar „Datenschutz in medizinischen Einrichtungen" bei der TÜV-Akademie Rheinland GmbH in Köln im Dezember 2011, Seminar „Datenschutz – Umstellung auf die EU-Grundverordnung (EU-DSGVO)" bei der TÜV Nord Akademie in Essen im Mai 2017, aktive Mitarbeit im ERFA-Kreis Sachsen/Deutschland für Datenschutzbeauftragte

5. Mitarbeiter der opta data Österreich GmbH

5.1 alle Mitarbeiter sind schriftlich zur Wahrung des Datengeheimnisses, der Schweigepflicht und der Vertraulichkeit nach DSGVO verpflichtet worden

5.2 die Verpflichtung erfolgte auf einem extra Formular

5.3 die der Verpflichtung zu Grunde liegenden Gesetzestexte wurden allen Mitarbeitern gegen Unterschrift ausgehändigt

5.4 die Verpflichtung wird bei Einstellung durch die Geschäftsleitung vorgenommen

5.5 alle Mitarbeiter werden in regelmäßigen Abständen durch die externe Datenschutzbeauftragte (eDSB) geschult – Schulungsnachweise sind vorhanden

6. Verzeichnis von Verarbeitungstätigkeiten/ Datenschutzfolgeabschätzung

6.1 das „Verzeichnis der Verarbeitungstätigkeiten" gem. Art. 30 DSGVO wird geführt und kann der zuständigen Aufsichtsbehörde für den Datenschutz zur Einsicht zugänglich gemacht werden

6.2 für Verfahren bei denen besondere Kategorien von Daten gem. Art. 9 Abs. 1 DSGVO (Gesundheitsdaten nach Art. 4 Nr. 15 DSGVO) verarbeitet werden, wird eine Datenschutzfolgeabschätzung durchgeführt

Version 8. Juli 2024

II. Technische und organisatorische Maßnahmen

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle)

Vertraulichkeit (Art. 32 Abs. 1 b) DSGVO)

1.1 Serverraum ist mit extra Schloss gesichert.

1.2 Zutritt zum Serverraum ist nur einem eingeschränkten Personenkreis möglich.

1.3 Räume in der 4. und 5. Etage sind mit nur einem Zugang ausgestattet.

1.4 Ergänzende Maßnahmen in der 5. Etage:

- Eingangstür aus Sicherheitsglas ist nur mit Token zu öffnen.
- Über den Aufzug ist die 5. Etage nur mit Token zu erreichen.
- Besucher müssen sich über ein im Aufzug befindliches Telefon anmelden und werden dann in die 5. Etage geholt.
- Rezeption ist während der Arbeitszeit immer beaufsichtigt.

1.5 Ergänzende Maßnahmen in der 4. Etage: Außerhalb der Dienstzeiten sind die Büroräumlichkeiten abgeschlossen.

1.6 Innerhalb der Dienstzeiten erfolgt eine Zugangskontrolle durch das Personal.

1.7 In den Räumlichkeiten erfolgt eine Begleitung betriebsfremder Personen durch Mitarbeiter.

1.8 Es gibt spezielle Arbeitsanweisungen für Mitarbeiter im Home-Office.

2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle)

Vertraulichkeit (Art. 32 Abs. 1 b) DSGVO

2.1 Daten in Papierform werden gesammelt und durch ein Entsorgungsunternehmen nach den Kriterien der ÖNORM S 2109-1 bzw. EN 15713 und ISO 21 964 vernichtet

2.2 elektronische und optische Datenträger werden selbst mechanisch vernichtet

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle)

Vertraulichkeit (Art. 32 Abs. 1 b) DSGVO)
Privacy by design / default (Art. 25 DSGVO)

3.1 Benutzername und Kennwort

3.2 Min. 12 Zeichen Passwortlänge bei Servern

3.3 Active Directory

3.4 Passwörter entsprechen in der Komplexität den Richtlinien des BSI

3.5 Standard Richtlinien von Microsoft - 8 Zeichen lang, besteht aus Klassen Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern – es müssen zumindest 3 Klassen verwendet werden.

3.6 An- und Abmeldungen werden protokolliert

3.7 gesicherte VPN- oder Citrix Zugänge für Mitarbeiter im Home-Office

3.8 keine lokale Datenhaltung für Mitarbeiter im Home-Office durch die Verwendung von Citrix

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle)

Integrität (Art. 32 Abs. 1 b) DSGVO)

4.1 gemanagte Firewalls

4.2 Verwaltung der VPN-Verbindung durch die od FIN

4.3 Fernwartung eigener Software nur über Teamviewer mit Sitzungsnummer und unter Aufsicht eines Mitarbeiters

4.4 alle E-Mails laufen über die Server der od FIN und werden dort auf Viren, Spam etc. überprüft

4.5 Übermittlungen zu den elektronischen Datensammelstellen der österreichischen Sozialversicherungsträger erfolgt verschlüsselt

5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle)

Vertraulichkeit (Art. 32 Abs. 1 b) DSGVO)

5.1 Serverraum nur mit extra kodierten Token zu öffnen (nur vier Personen haben Zugang)

5.2 extra Administrationspasswörter für die Server

5.3 je nach Softwarelösung wird zur Authentifizierung ein/e Mitarbeiterkennung/Passwort bzw. Benutzername/Kennwort verlangt

5.4 Vergabe von Benutzerrechten erfolgt auf schriftlichen Antrag

5.5 verschiedene Benutzerhierarchie

Version 8. Juli 2024

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle)

Integrität (Art. 32 Abs. 1 b) DSGVO)

6.1 VPN Verbindungen werden nur auf Antrag (schriftliches Formular) frei geschaltet

6.2 Übermittlungsprotokolle und Meldebestätigung bei Übertragungen zu österreichischen Sozialversicherungsträgern

7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle)

Integrität (Art. 32 Abs. 1 b) DSGVO)

7.1 durch Protokolle im Active Directory

7.2 durch Anwendungsprotokolle

7.3 durch Protokolle bei Änderung von Daten (Erfassung)

8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle)

Vertraulichkeit (Art. 32 Abs. 1 b) DSGVO)
Integrität (Art. 32 Abs. 1 b) DSGVO)

8.1 kein Transport von Datenträgern außer Haus

8.2 Datenträger zur Datensicherung verbleiben auch im Haus

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit)

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b) DSGVO)

9.1 Aufstellung aller physikalischen und virtuellen Server sowie Netzwerkpläne vorhanden

9.2 alle Server sind mit Raid-Systemen ausgestattet, die die Daten permanent spiegeln

9.3 Datensicherungskonzept

9.4 Notfallkonzept

9.5 automatisiertes Backupverfahren (verschiedene Datenbestände)

10. Gewährung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b) DSGVO)

10.1 Raid-Systeme melden Plattenausfälle in den Servern

10.2 Virenscanner mit automatischem Updaten über das Internet

10.3 Filterung und Scan von eingehenden und ausgehenden E-Mails

10.4 Serverraum mit Klimaanlage, Feuerlöscher und Rauchmelder

11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)

Integrität (Art. 32 Abs. 1 b) DSGVO)

11.1 Trennung von Produktiv- und Testsystemen über die Entwicklung der od FIN

12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle) Verfahren zur regelmäßigen Evaluierung der TOM´s gem.

Art. 32 Abs. 1 d) und Art. 25 Abs. 1 DSGVO

12.1 durch Verträge gem. Art. 28 und 29 DSGVO

12.2 durch die Einräumung von Kontrollrechten für Auftraggeber

12.3 durch Schulung der Mitarbeiter

12.4 durch schriftliche Anweisungen die jeder Mitarbeiter unterschrieben hat

12.5 durch regelmäßige Audits der ext. Datenschutzbeauftragten

13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle) Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b) DSGVO)

13.1 alle Server sind an unterbrechungsfreie Stromversorgung (USVs) angeschlossen

13.2 Serverraum mit Klimaanlage, Rauchmelder und Feuerlöscher

13.3 Sicherungsmedien lagern in einem anderen Brandabschnitt als der Serverraum

14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit)

Integrität (Art. 32 Abs. 1 b) DSGVO)

14.1 durch interne Mandantenfähigkeit und Authentifizierung der Kunden bzw. Auftraggeber

14.2 Systeme sind auf mehrere Server verteilt

Version 8. Juli 2024