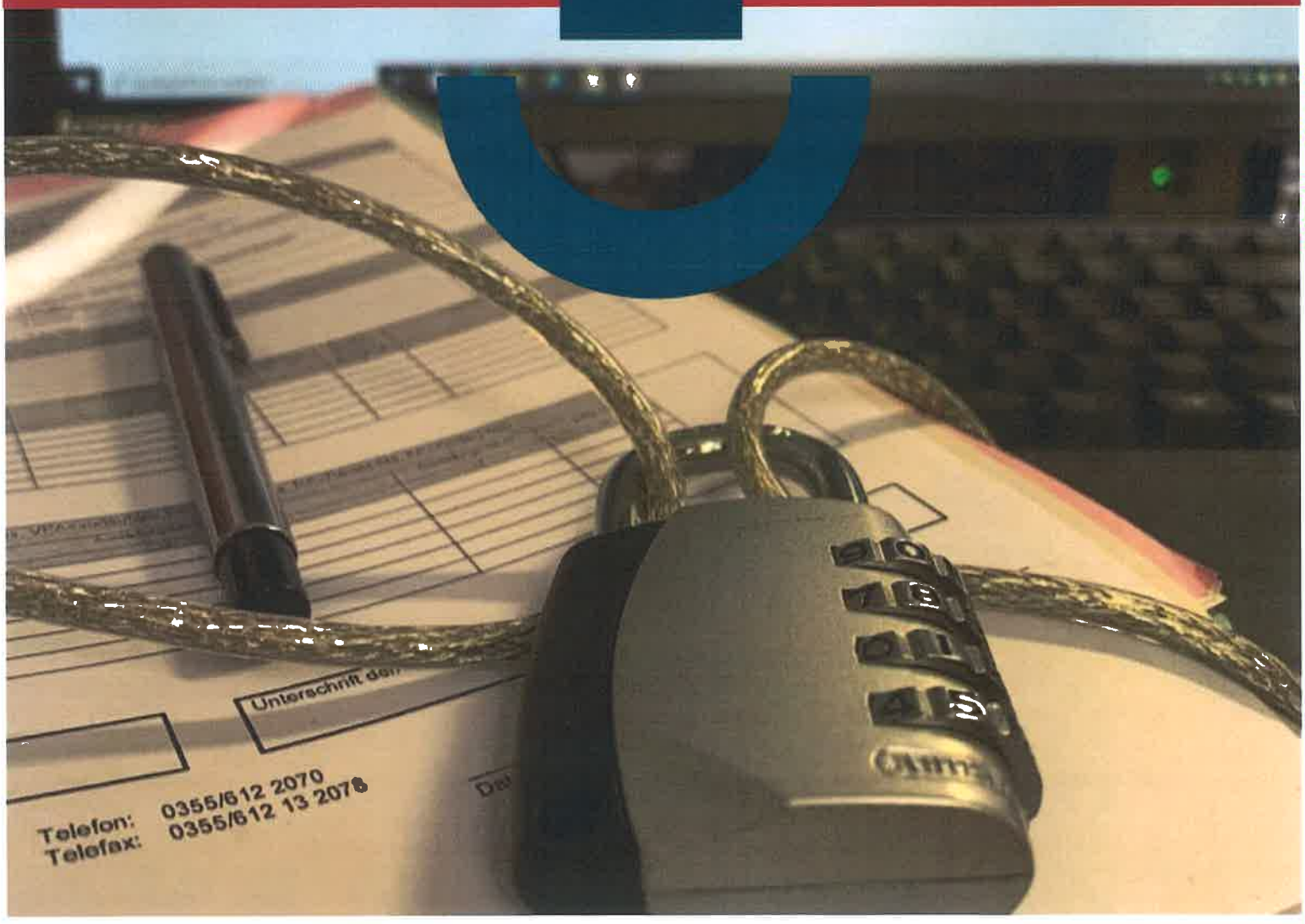
DATENSCHUTZKONZEPT

ADOPTIONSVERMITTLUNGSSTELLE LANDKREIS SPREE-NEIßE (WOKREJS SPRJEWJA-NYSA) UND STADT COTTBUS/CHÓŚEBUZ



Auftraggeberin:

Stadt Cottbus/Chóśebuz
Neumarkt 5
03046 Cottbus

Autor:

Theodor Kubusch
Datenschutz- und Informationssicherheitsbeauftragter

Stadt Cottbus/Chóśebuz
Büro des Oberbürgermeisters
Neumarkt 5
03046 Cottbus

Tel. 0355-612 2126
Fax 0355-612 13 2126
E-Mail: datenschutz@cottbus.de
Internet: www.cottbus.de/datenschutz

Fassung:

Version V 0.1 [ENTWURF] | TK | 04/2021

Sicherheitsklassifizierung:

Das Dokument ist für internen Gebrauch der Stadt Cottbus/Chóśebuz und des Landkreises Spree-Neiße (Wokrejs Sprjewja-Nysa) bestimmt. Weitergaben an Dritte, Veröffentlichungen – auch in Teilen – sind mit dem Urheber abzustimmen.

Inhaltsverzeichnis

Analgenverzeichnis

1 Präambel

Die Stadt Cottbus/Chóśebuz führt für den Landkreis Spree-Neiße (Wokrejs Sprjewja-Nysa) die Aufgabe der Adoptionsvermittlungsstelle gemäß § 2 AdVermiG auf Grundlage einer mandatierenden öffentlich-rechtlichen Vereinbarung durch. Hierbei verarbeitet sie eine Vielzahl personenbezogener Daten auf Grundlage eines Vertrags zur Auftragsverarbeitung (Art. 28 DSGVO). Gemäß Art. 28 Abs. 3 lit. d DSGVO hat die Stadt Cottbus/Chóśebuz alle technischen und organisatorischen Maßnahmen zu ergreifen, um die Sicherheit bei der Verarbeitungstätigkeit für den Landkreis Spree-Neiße (Wokrejs Sprjewja-Nysa) gewährleisten zu können. Die Vorgaben dieser Maßnahmen ergeben sich aus den Vertragswerken, insbesondere aus den technischen und organisatorischen Maßnahmen (TOM) i. S. d. Art. 32 DSGVO für Datenverarbeitung Adoptionsvermittlungsstelle Landkreis Spree-Neiße (Wokrejs Sprjewja-Nysa) i. d. F. v. 10.03.2021, Version 1.0.

Das vorliegende Datenschutzkonzept dient als Nachweis, die vom Landkreis Spree-Neiße (Wokrejs Sprjewja-Nysa) vorgesehenen Anforderungen durch entsprechende Maßnahmen umgesetzt zu haben. Zudem dient das Konzept der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO).

2 Maßnahmen

2.1 Vertraulichkeit

2.1.1 Zutrittskontrolle

2.1.1.1 Manuelle Schließsystem

Die Stadt Cottbus/Chóśebuz verfügt in dem betreffenden Bereich über ein manuelles Schließsystem. Die Schlüsselverwaltung erfolgt auf Grundlage der Dienstanweisung Schlüsselordnung (DA II_10_11).

Anzumerken ist, dass das Schließsystem über keinen ausreichenden patentrechtlichen Schutz mehr verfügt (Ablauf 2015) und dahingehend im Schutzniveau geschwächt ist. Der technische Kopierschutz sei hingegen gegeben. Weiter ist darauf hingewiesen, dass durch Verlust eines Generalschlüssels nicht auszuschließen ist, dass das Sicherheitssystem kompromittiert sein könnte.

2.1.1.2 Besucherbegleitung

Eine durchgängige Besucherbegleitung im gesamten Objekt ist nicht gewährleistet. Jedoch dürfen sich fremde Personen nicht unbeaufsichtigt in Büro- oder sonstigen Räumen, in denen personenbezogene Daten aufbewahrt werden, verweilen (Punkt 6.1 Abs. 3 S. 4 und Abs. 5 Dienstanweisung Datenschutz und Informationssicherheit (DA II_01_6)).

2.1.1.3 Sorgfaltspflicht Auswahl Sicherheitspersonal

Die Auswahl der Sicherheitsdienstleister/-innen erfolgt nach den gängigen vergaberechtlichen Kriterien der Zuverlässigkeit und Leistungsfähigkeit. Die Sicherheitsdienstleister/-innen werden durch Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO an die Anforderungen der Stadt Cottbus/Chóśebuz gebunden.

2.1.1.4 Sorgfaltspflicht Auswahl Reinigungspersonal

Die Auswahl der Reinigungsdienstleistungsunternehmen erfolgt nach den gängigen vergaberechtlichen Kriterien der Zuverlässigkeit und Leistungsfähigkeit. Verträge zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO werden regelmäßig nicht geschlossen, da Reinigungspersonal keinen Zugang zu bzw. Zugriff auf personenbezogene Daten erhält und somit keine Auftragsverarbeitung stattfindet. Hierzu werden die Sicherheitsmaßnahmen des unbeaufsichtigten Verweilens fremder Personen und dauerhaften Verschließens personenbezogener Daten und sonstiger sensibler Informationen in Aktenschränken (Punkt 6.1 Abs. 3 S. 4 und Abs. 5 DA II_01_6), zu denen das Reinigungspersonal keinen Zugang hat, als Gegenmaßnahmen als ausreichend angesehen.

2.1.1.5 Weiterführende Maßnahmen

Das Objekt, in dem die Adoptionsvermittlungsstelle angesiedelt ist, wird durch Videoüberwachungsmaßnahmen geschützt. Ferner befindet sich ein Pfortendienst im Objekt. Als Zutrittskontrolle sind Maßnahmen zur Sichtauthentifizierung (Dienstausweise) und ein Anmeldemanagement etabliert.

Der Auftragsverarbeiter für IT-Dienstleistungen (DIKOM) ist durch Vertrag zur Auftragsverarbeitung (Art. 28 Abs. 3 DSGVO) an die Regelungen der Stadt Cottbus/Chóśebuz gebunden. Die Sicherheitsmaßnahmen richten sich nach dem BSI-Standard 200-2, die u. a. Zutrittssicherheitsregelungen umfassen.

2.1.2 Zugangskontrolle

2.1.2.1 Identitäts- und Berechtigungsmanagement

2.1.2.1.1 Authentisierung (Benutzername, Passwort)

Die Stadt Cottbus/Chóśebuz ist an die BSI-Standards 200-1 bis 200-3 gebunden (§§ 12, 16 BbgEGovG). Diese umfassen Anforderungen an ein Identitäts- und Berechtigungsmanagement (ORP.4 IT-Grundschutz-Kompendium), welches für die Systemzugänge zu den IT-Komponenten flächendeckend im betreffenden Bereich durch verschiedene An- und Abmeldeprozesse gewährleistet ist (Fachbereich Verwaltungsmanagement). Als Authentisierungsmittel kommt eine Benutzername-Passwort-Kombination zum Einsatz.

2.1.2.1.2 Berechtigungsverwaltung

Die Zuweisung und Entziehung von Rollen und Rechten erfolgt gegenüber dem externen IT-Dienstleister durch betriebsüblichen Ticket-Prozess, der durch die zugrundeliegenden Verträge zur Auftragsverarbeitung geregelt ist.

2.1.2.1.3 Passwortkonvention

Zum gegenwärtigen Zeitpunkt gilt als Passwortkonvention gemäß Dienstanweisung IT-Arbeitsplatz, Punkt 8 der Richtlinie IT-Nutzung für die Systemzugänge eine Mindestlänge von 15 Stellen (geplant Kürzung auf 12 Stellen). Zur Gewährleistung der Komplexität soll das Passwort mindestens drei der vier gängigen Kategorien (Großbuchstaben, Kleinbuchstaben, Sonderzeichen, Ziffer) umfassen. Ein regelmäßiger Wechsel ist, entsprechend h. M. (vgl. ORP.4.A22, A23 IT-Grundschutz-Kompendium) nicht vorgesehen.

Andere Passwörter (bspw. Fachanwendungen), die nicht den Anforderungen entsprechen, sollen zukünftig durch Auffangnorm der DA II_01_6 entsprechend der Anforderungen des ORP.4 (bspw. durch regelmäßigen Wechsel) als sichere Passwörter gestaltbar gemacht werden.

2.1.2.2 Anti-Viren-Software (Server, Clients, mobile Endgeräte)

Sämtliche IT-Komponenten sind mit entsprechender Anti-Viren-Software ausgestattet. Die Stadt Cottbus/Chóśebuz betreibt selbst keine Server- und Client-Technik in eigener Verantwortung und hat per Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO die Anforderung an den DIKOM delegiert. Die Endgeräte sind mit Trend Micro Security Agent versehen, was einen zuverlässigen Anti-Viren-Schutz gewährleistet.

Mobile Endgeräte, sofern Sie als Clients betrieben werden (Notebooks, Tablets) werden nach den Client-Anforderungen behandelt.

Smartphones werden per Mobile-Device-Management (MDM) verwaltet. Da für die (ausnahmslos) betriebenen iPhones mit iOS keine sinnvollen Einsatzgebiete mit Anti-Viren-Software gegeben sind, erfolgt kein gesonderter Einsatz auf den Endgeräten. Die damit verbundenen Risiken wurden in einer Beurteilung des MDM bewertet und übernommen.

2.1.2.3 Firewall

Die Stadt Cottbus/Chóśebuz betreibt keine eigenen Firewalls in dem betreffenden Arbeitsgebiet. Die Anforderungen an sichere Firewalls (NET.3.2 IT-Grundschutz-Kompendium) sind auf den Auftragsverarbeiter gemäß Vertrag nach Art. 28 Abs. 3 DSGVO übertragen. Es sind entsprechende Firewalls und Firewall-Konzepte im Einsatz.

2.1.2.4 Intrusion-Detection-System

Die im Einsatz befindliche Anti-Viren-Software (Trend Micro Security Agent) umfasst Elemente eines Intrusion-Detection-System. Die Angriffserkennung ist im Sinne der Auftragsgeberin ausreichend.

2.1.2.5 Verschlüsselung Datenträger

Alle mobilen Endgeräte sind durch technische Voreinstellung mit einer Datenträgerverschlüsselung vorgesehen. Notebooks werden durch technische Administration des vertraglich gebundenen Auftragsverarbeiters nur Endgeräteverschlüsselt ausgegeben. Die Prozesse einschließlich Test- und Abnahmeverfahren sind einschlägig geregelt. Smartphones werden per MDM mit der iOS-Verschlüsselung voreingestellt und unveränderbar verschlüsselt.

Sonstige hardwareverschlüsselte Datenträger (USB-Sticks) werden durch die Fachbereiche dezentral verwaltet. Es gelten organisatorische Regelungen, dass andere, als hardwareverschlüsselte Datenträger, nicht genutzt werden dürfen, um personenbezogene Daten oder andere sensitive Informationen zu speichern (Punkt 16 DA IT-Arbeitsplatz, Punkt 6.2.6 DA II_01_6).

2.1.2.6 Verschlüsselung Smartphones

Smartphones werden durch administrative Vorgaben per MDM ausschließlich verschlüsselt betrieben (vgl. Nr. 28 lit. b Sicherheitsrichtlinie Smartphones).

2.1.2.7 Sperre externe Schnittstelle (USB)

Die organisatorischen Regelungen verbieten den Anschluss privater Endgeräte via USB (Punkt 11 RL IT-Nutzung, Punkt 6.2.1 lit. d DA II_01_6).

2.1.2.8 Automatische Desktopsperre

Beim Verlassen des IT-Arbeitsplatzes ist der Bildschirm zu sperren (Punkt 13 RL IT-Nutzung). Es ist sicherzustellen, dass Regelungen über den Zugang zu IT-Systemen geschaffen werden, die auch Regelungen über die manuelle Sperrung von IT-Geräten durch den Beschäftigten einschließen. Die Zeit bis zur automatischen Sperre soll 10 Minuten nicht überschreiten (Punkt 14 RL IT-Nutzung).

2.1.2.9 Verschlüsselung Notebooks/Tablets

Notebooks und Tablets werden ausschließlich verschlüsselt (Full Disk Encryption) ausgegeben, sofern es sich bei den Endgeräten über Lenovo ThinkPads handelt, die über den DIKOM beschafft, verwaltetet und ausgegeben werden. Dies ist der Regelfall, jedoch ist nicht lückenlos ausgeschlossen, dass andere Geräte eingesetzt werden. für den Bereich der Adoptionsvermittlung ist durch den Fachbereich 51 Jugendamt zu regeln, dass ausschließlich die o. g. Geräte eingesetzt werden. Die Verschlüsselung erfolgt durch die BIOS-gestützte FDE-Lösung, für die ein Festplattenkennwort (vier Ziffern) festgelegt ist, welches nur den Nutzer/-innen bekannt ist. Ein regelmäßiger Wechsel ist nicht etabliert. Das Masterpasswort ist ausschließlich dem DIKOM bekannt.

Eine Nutzung von Notebooks/ Tablets ist für die Adoptionsvermittlungsstelle aktuell nicht vorgesehen.

2.1.2.10 Löschen und Vernichten

Die Stadt Cottbus/Chóśebuz verfügt über kein vollständiges Lösch- und Vernichtungskonzept. Die Löschung elektronischer Endgeräte, die über den DIKOM bereitgestellt werden, erfolgt nach dem vertraglich vereinbarten Mindeststandard DIN 66399 Schutzklasse 2, Sicherheitsstufe 4, insb. durch Standard DoD 5220.22-M.

Für die Vernichtung papiergebundener Datenträger sind ausschließlich Aktenvernichter – oder sofern Dienstleistungsunternehmen nach Art. 28 DSGVO beauftragt werden – einzusetzen, die nach DIN 66399 die Schutzklasse 2, Sicherheitsstufe 4 erfüllen. Zum gegenwärtigen Zeitpunkt erfolgt die Vernichtung per Aktenvernichter IDEAL 4002 CC mit Sicherheitsstufe P-4 (4 x 40 mm), der die Anforderung erfüllt. Die gemäß Art. 28 Abs. 3 DSGVO gebundene Auftragnehmerin, die mit der Vernichtung großer Mengen beauftragt ist, vernichtet die Unterlagen nach DIN 66399 P-3, die durch Verwirbelungstechnik Sicherheitsstufe P-4 erfüllt.

2.1.3 Zugriffskontrolle

Externer Aktenvernichter

Siehe Kapitel 2.2.10: Die externe Aktenvernichterin ist durch Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO vertraglich gebunden. Erkenntnisse über Zertifizierungen, insbesondere nach DIN 66398 und 66399 liegen keine vor. Die Verbringung und Vernichtung des Schriftgutes werden in dieser Form von der Auftraggeberin anerkannt.

2.1.4 Trennungskontrolle

Es wurden keine Maßnahmen durch den Auftraggeber festgelegt.

Die Trennung zwischen personenbezogenen Daten des Auftraggebers und der Auftragnehmerin erfolgt nach logischer Zuordnung in gesonderten Akten und Aufbewahrungsbehältnissen.

2.1.5 Pseudonymisierung und Verschlüsselung

Es wurden keine Maßnahmen durch den Auftraggeber festgelegt.

Pseudonymisierung und Verschlüsselung werden in betrieblicher Übung eingesetzt.

Also Verschlüsselungsmöglichkeiten für digitalen Schriftverkehr stehen der Auftragnehmerin S/MIME, ein HTTPS-verschlüsselter Transferserver sowie verschlüsselte Dokumenten-Anhänge zur Verfügung.

2.2 Integrität

2.2.1 Weitergabekontrolle

2.2.1.1 Einsatz von VPN

Sofern Zugriffe auf das virtuelle Systeme der Auftragnehmerin von außen erforderlich sind, werden diese ausschließlich per VPN zugelassen. Die Zugriffe erfolgen nach betrieblicher Übung. Der Aufbau eines entsprechenden Regelwerkes und die Etablierung notwendiger Prozesse befinden sich seit geraumer Zeit im Aufbau. Die bestehenden Regelungen werden von der Auftraggeberin anerkannt. Zugriffe auf die Exchange-Server (Sync per Smartphones) erfolgt ausschließlich per Mobile-Device-Management gemäß Sicherheitsrichtlinie Smartphones.

2.2.1.2 Sichere Transportbehälter

Der Fachbereich 51 Jugendamt verfügt gegenwärtig über einen sicheren Transportbehälter. Grundsätzlich ist die Aktenverbringung untersagt, sofern die Natur des Geschäftsgangs oder andere Notwendigkeiten dies nicht unabdingbar machen (Punkt 6.1 Abs. 6 DA II_01_6). Sofern die Verbringung von Schriftgut erforderlich werden sollte, ist eine solche nur nach den Vorgaben der Datenschutz- und Informationssicherheitsrichtlinie „Aktenverbringung“ zulässig.

2.2.2 Eingangskontrolle

Es wurden keine Maßnahmen zur Eingangskontrolle durch den Auftraggeber festgelegt.

2.3 Verfügbarkeit und Belastbarkeit (Verfügbarkeitskontrolle)

2.3.1 Feuer- und Rauchmeldeanlage

Das Objekt ist mit einer Sprinkler-Löschanlage, Handfeuermelde-Anlage, Rohr- und Düsensystem, Brandmeldeanlagen (automatische Brandmelder, Handfeuermelder, Alarmsirenen, elektroakustische Alarmierungseinrichtungen, Lautsprecher) versehen (Brandschutzordnung Spree-Galerie Cottbus).

2.3.2 Backup- und Recovery-Konzept

Der DIKOM ist per Vertrag zur Auftragsverarbeitung nach Art. 28 Abs. 3 DSGVO zur Gewährleistung von Datensicherungsmaßnahmen verpflichtet. Hierzu liegt ein Datensicherungskonzept zu Grunde (EVB-IT-Servicevertrag SVC-DIKOM-2020/07 v. 21.02.2021, Leistungsbeschreibung, Kapitel 2.1.15 sowie Anlage „Datensicherungskonzept"). Das Konzept umfasst eine Backupstrategie.

2.4 Verfahren zur Überprüfung, Bewertung und Evaluierung

2.4.1 Datenschutz-Maßnahmen

2.4.1.1 Wirksamkeitsprüfung

Es sind keine Prozesse zur Umsetzung der Wirksamkeitsprüfung etabliert.

2.4.1.2 Datenschutzbeauftragter

Die Stadt Cottbus/Chóśebuz hat einen Datenschutzbeauftragten benannt:

vgl. www.cottbus.de/datenschutz

2.4.1.3 Schulungsmaßnahmen

Vor der ersten Verarbeitungstätigkeit jeder/-s Beschäftigten ist eine Verpflichtung auf den Datenschutz gemäß Art. 29 DSGVO durchzuführen (Punkt 5.5.1 Abs. 1 DA II_01_6). Für den betreffenden Bereich erfolgt dies durch sogenannten „Laufzettel-Prozess" des Fachbereichs 11 Personal- und Organisationsmanagement durch den Datenschutz- und Informationssicherheitsbeauftragten.

Ferner haben die jeweiligen Bereiche den erforderlichen Schulungsbedarf zum Datenschutz zu ermitteln und entsprechende Schulungsangebote zu etablieren und zu unterbreiten. Das zentrale Seminarangebot der Stadt Cottbus/Chóśebuz sieht allgemeine Datenschutzschulungen für alle Beschäftigten vor (Seminarkatalog 2021, Kapitel 8, DS 1 bis DS 4). Die Inanspruchnahme der Angebote obliegt den Fachbereichen bzw. den jeweiligen Beschäftigten.

Der Fachbereich 51 Jugendamt etabliert gegenwärtig ein eigenes Seminarkonzept zum Datenschutz, welches im regelmäßigen Wechsel zu verschiedenen Datenschutzthemen sowohl intern als auch extern angeboten werden soll.

2.4.1.4 Sensibilisierungsmaßnahmen

Die Anforderungen des Datenschutzes werden während der Einarbeitung neuer Beschäftigter berücksichtigt.

Ferner erfolgt die Vermittlung wesentlicher oder anlassbezogener Ansätze in den Dienstberatungen.

Auf dem gemeinsamen Laufwerk befinden sich Datenschutzhinweise im Qualitätshandbuch sowie in den jeweils zutreffenden Datenschutzdokumentationen.

Zentrale Hinweise, Anregungen und Empfehlungen werden unverzüglich an die Beschäftigten über- und im Bedarfsfall gesondert vermittelt.

2.4.1.5 Informationssicherheitsbeauftragter

Die Stadt Cottbus/Chóśebuz hat einen Informationssicherheitsbeauftragten benannt. Diese Funktion wird durch den Datenschutzbeauftragten in Personalunion wahrgenommen (vgl. Punkt 3.1 DA II_01_6).

2.4.1.6 Datenschutz-Folgenabschätzung

Sofern der Auftraggeber die Durchführung einer DSFA für erforderlich erachtet, wird die Auftragnehmerin die dafür notwendigen Informationen an den Auftraggeber übergeben. Die Verantwortung für die Durchführung, insbesondere Analysen, Bewertungen und erforderliche Maßnahmen verbleiben im Auftragsverhältnis bei dem Auftraggeber.

2.4.1.7 Informationspflichten Artt. 13, 14 DSGVO

Die Auftragnehmerin hat einen gängigen Prozess zur Einhaltung der Pflichtinformationen nach Artt. 13, 14 DSGVO etabliert. Die Informationen werden, sofern vorhanden, unter www.cottbus.de/datenschutz > Informationspflichten veröffentlicht. Sobald der Auftraggeber die notwendigen Informationen zur Verfügung stellt, werden diese dort veröffentlicht oder auf den Seiten des Auftraggebers verlinkt.

2.4.1.8 Prozess Betroffenenrechte

Für die Geltendmachung der Betroffenenrechte sind keine konkreten Regelungen etabliert. Es gelten insofern die abstrakten Regelungen nach Punkt 6.6 DA II_01_6. Somit sind solche Verlangen durch den Fachbereich 51 Jugendamt dezentral zu bearbeiten.

2.4.2 IT-Störungsmanagement

2.4.2.1 Firewall

Der DIKOM ist als Auftragnehmer per Vertrag nach Art. 28 Abs. 3 DSGVO zum Betrieb einer Firewall verpflichtet. Zum Einsatz kommt eine Firewall-Lösung der Barracuda Networks Inc.

2.4.2.2 Spamfilter

Der DIKOM ist als Auftragnehmer per Vertrag nach Art. 28 Abs. 3 DSGVO zum Betrieb eines Spamfilters verpflichtet. Der SMILTER ist in der Firewall-Lösung integriert.

2.4.2.3 Virenscanner

Der DIKOM ist als Auftragnehmer per Vertrag nach Art. 28 Abs. 3 DSGVO zum Betrieb eines Virenscanners verpflichtet. Zum Einsatz kommt der Apex One Security Agent von Trend Micro.

2.4.2.4 Sicherheitsvorfälle

Für die Erkennung, Meldung, den Umgang, die Einbindung entsprechender Stellen, Dokumentation und Nachbearbeitung von Sicherheitsvorfällen kommt ein zentraler Prozess zur Anwendung. Meldepflichten ergeben sich dabei aus Punkt 5.1 Abs. 3 und Punkt 6.3 der DA II_01_6 sowie das konkrete Vorgehen aus der darauf basierenden Datenschutzrichtlinie Datenschutzverletzung.

Zudem ist gegenwärtig der Aufbau eines internen Computer-Ereignis- und Reaktions-Teams (CERT_intern) in Planung (Entwurf 1.0.5 zu Punkt 6.3 DA II_01_6 zur Umsetzung des § 16 Abs. 2 S. 3, 4 BbgEGovG), welches die Vorgaben ergänzt bzw. eventuelle Melde- und Behebungslücken schließen soll.

2.4.3 Datenschutzfreundliche Voreinstellungen

2.4.3.1 Datenminimierung

Der Datenminimierungsgrundsatz ist als Grundsatz durch Punkt 4.2 DA II_01_6 im Allgemeinen etabliert. Die praktische Umsetzung und der Erlass entsprechender Regelungen in der konkreten Arbeitsweise obliegt dem Fachbereich 51 Jugendamt.

2.4.3.2 Widerrufsrecht

Erfolgt die Verarbeitung personenbezogener Daten ausnahmsweise auf Grundlage einer Einwilligung, so ist der gesetzlich vorgesehene Widerrufsprozess einzuräumen. Da die Einwilligungslösung im hoheitlichen Handeln als Ultima ratio gilt, erfolgen keine tiefgreifenden zentralen Regelungen dazu. Der Fachbereich 51 Jugendamt hat Einwilligungslösungen an den verbindlich angeordneten Empfehlungen nach Anlage 1 zur DA II_01_6 zu etablieren.

2.4.4 Auftragskontrolle

Es wurden keine Maßnahmen zur Auftragskontrolle durch den Auftraggeber festgelegt.

Cottbus, ...

Fachbereich 51 Jugendamt