Technische und organisatorische Maßnahmen, Art. 32 DSGVO

I. Vertraulichkeit

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

Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen der Stadt Weilheim erlangen:

- Der Zutritt zu den Räumlichkeiten und damit zu den Arbeitsplatzrechnern und Servern ist über eine kontrollierte und protokollierte Schlüsselvergabe (Schließanlage) gewährleistet.
- Die Räume sind grundsätzlich verschlossen oder durch Mitarbeiter besetzt. Türen und Fenster sind außerhalb der Geschäftszeiten immer verschlossen.
- Der Zutritt für Besucher zu den Diensträumen wird durch eigenes Personal kontrolliert.
- Foyer, Treppenhaus und Tiefgarage werden mit Überwachsungskameras überwacht. Die Aufzeichnungen werden 72 Stunden aufbewahrt.
- Die Server der Stadtverwaltung Weilheim stehen in einem gesondert abgeschlossenen Raum, zu dem nur Mitarbeiter mit einem Generalschlüssel Zutritt haben.
- Die Datensicherung erfolgt täglich auf einem Disk-to-Disk-to-Tape System in einem separaten Gebäude der Stadtverwaltung. Die wöchentlichen Tape-Sicherungen werden in einem weiteren abgeschlossenen Raum verwahrt, zu dem nur Personen mit Generalschlüssel Zutritt haben.
- Die Datenverarbeitung erfolgt überwiegend in dem von der Stadt Weilheim beauftragten Rechenzentrum (ITEOS, Krailenshaldenstraße 44, 70469 Stuttgart). Diese haben ein umfassendes Konzept zum Schutz der Daten vor unbefugtem Zutritt. Andere Auftragnehmer zur Datenverarbeitung haben einen Auftrag zur Datenverarbeitung vorgelegt und darin ein schlüssiges Konzept zur Zutrittskontrolle vorgelegt.
- Personenbezogene Daten werden nicht außerhalb gesicherter Rechenzentren gespeichert.

Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

- Der Zugang zu Endgeräten von Mitarbeitern wird durch Betriebssystemkennung und ein persönliches Passwort geschützt. Benutzerkonten sind nur einer Person zugeordnet.
- Die Passwortkomplexität und –länge gemäß BSI Empfehlung wird systemseitig erzwungen.
- Nach einer bestimmten Zahl erfolgloser Login-Versuche wird der Zugang gesperrt und kann nur vom Administrator entsperrt werden.
- Der Zugang von außen auf das Netz des Auftragnehmers wird durch verschlüsselte Verbindungen (VPN-Tunnel mit Benutzername und Kennwort) oder Verbindungen über getunnelte RDP-Sitzungen mit zwei Faktor-Authentifizierung mit Benutzername, Kennwort und einmal TAN sichergestellt.
- Mitarbeiter erhalten nur im Rahmen Ihrer Tätigkeit Zugriff auf die notwendigen Systeme und Daten.
- Standarduser erhalten keine Administrationsrechte.
- Einrichtung und Änderung von Benutzerkonten erfolgt zentral durch die IT Stelle. Bei Austritt eines Mitarbeiters werden alle zugehörigen Benutzerkonten gelöscht.
- Nach fünf Minuten Inaktivität wird der Bildschirm gesperrt und ist nur durch Eingabe des Windows-Kennwort zu entsperren.

Zugriffskontrolle

Folgende implementierte Maßnahmen gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

- Soweit technisch machbar, werden An- und Abmeldungen der Benutzer an den DV-Arbeitsstationen und den Anwendungen protokolliert. Internetzugriffe und Mailverkehr werden datenschutzkonform protokolliert. Eine Auswertung erfolgt zur technischen Fehleranalyse oder Verdacht eines Richtlinienverstoßes.

- Im Rahmen des technisch und organisatorisch Machbaren sind angemessene Abstufungen der Zugriffsberechtigten aufgebaut. Diese erlauben das Eingeben, Lesen, Kopieren, Verändern oder Entfernen von personenbezogenen Daten bei der Verarbeitung, Nutzung und nach der Speicherung nur in dem für die jeweilige Aufgabe erforderlichen Umfang. Die Zugriffsberechtigten werden durch den Systemadministrator verwaltet.

- Die Aufbewahrung von Sicherungsdatenträgern erfolgt in verschlossenen Räumen, zu denen nur das betroffene Betriebspersonal und Personen mit Generalschlüssel Zutritt haben.

- Ausgemusterte Datenträger werden datenschutzgerecht vernichtet. Die Vernichtung wird dokumentiert und zertifiziert.

- Das Netzwerk der Stadt Weilheim ist durch eine zentrale Firewall geschützt.

- Alle Mitarbeiterrechner und Server sind mit Antivirensoftware geschützt.

- Updates der Betriebssysteme und Antivirensoftware werden vom Server zentral bereitgestellt.

- Eine Deaktivierung der Antivirensoftware, der Firewall oder der Sicherheitsupdates ist ohne Administrationsrechte nicht möglich.

- Werden Notebooks eingesetzt, werden alle Daten darauf verschlüsselt. Zum Einsatz kommt BitLocker oder ein vergleichbares Programm.

- Fernwartung findet nur über die vom Systemadministrator freigegebene Software unter Aufsicht des jeweiligen Mitarbeiters statt.

Trennungskontrolle

Folgende implementierte Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Die Stadt Weilheim setzt für die personenbezogene Datenverarbeitung getrennte Verfahren (beispielsweise Einwohnerwesen, Liegenschaften, Steuern etc.) ein. Die Daten werden getrennt erhoben, verarbeitet und gespeichert.

- Die Nutzeraccounts sind auf einzelne Verfahren beschränkt

- Die Stadt Weilheim nutzt personenbezogene Daten nur im Rahmen der Aufgabenerfüllung oder der hoheitlichen Tätigkeit. Die Daten werden entsprechend des Zwecks getrennt gespeichert. Alle Mitarbeiter sind angewiesen und werden regelmäßig geschult, Daten nur im Rahmen der

Dienstleistungserbringung und zur Wahrung der Zweckbindung zu erheben, zu verarbeiten und zu nutzen.

II. Integrität

(Art. 32 Abs 1 lit. b DSGVO)

Weitergabekontrolle
Folgende implementierte Maßnahmen gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Externer Zugriff auf die Server der Stadtverwaltung (Beispiel Telearbeit) erfolgt über eine verschlüsselte VPN-Verbindung über Watchguard oder über eine getunnelte RDP-Sitzung über Pintexx mit 2-Faktor-Autentifizierung (Kennwort und einmal TAN).

- Defekte oder ausgemusterte Datenträger werden revisionssicher vernichtet. Der Dienstleister bescheinigt mit Datum und Seriennummer die Vernichtung.

- Der Datenaustausch mit anderen Behörden erfolgt über das gesicherte Landesverwaltungsnetz

- Der Transport von Sicherungsdatenträgern, die personenbezogene Daten enthalten, erfolgt ausschließlich durch besonders ausgewählte und eingewiesene Mitarbeiter des Auftragnehmers.

- Die Stadt Weilheim unterhält ein Behördenkonto (beBPo) über Service-BW zur gesicherten Kommunikation mit Unternehmen und Bürgern.

- Cloud-Dienste wie Dropbox, WeTransfer, Microsoft OneDrive etc. werden nicht genutzt.

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

- Die Eingabe wird innerhalb des CMS Dokumentiert. Änderungen können Nachverfolgt und Rückgängig gemacht werden.

- Die Verfahren des Kommunalen Rechenzentrums zur Verarbeitung personenbezogener Daten protokollieren Änderungen in den Datensätzen.

Auftragskontrolle

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

- Mit sämtlichen Auftragnehmern zur Verarbeitung von personenbezogenen Daten der Stadt Weilheim wurde jeweils ein schriftlicher Vertrag zur Auftragsdatenverarbeitung geschlossen.

III. Verfügbarkeit, Belastbarkeit

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

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind bzw die Daten wiederhergestellt werden können:

- Die Stadt Weilheim rüstet ihre relevanten DV-Systeme mit einem geeigneten Schutz gegen Viren, Trojaner, Würmer und sonstige Malware aus und gewährleistet dadurch einen hinreichenden Schutz gegen Verletzung der Systemintegrität durch die vorgenannten Gefahren.

- Die Ausführung arbeitsplatzfremder Software wird, soweit technisch möglich, durch technische Maßnahmen und durch organisatorische Regelung verhindert.

- Betriebssysteme und Schutzsoftware werden in angemessenen Zeitabständen aktualisiert. Für Windows Betriebssysteme werden die Updates durch Windows Server Update Service zentral ausgerollt.

- Zum Schutz der zentralen DV-Anlage steht eine unterbrechungsfreie Stromversorgung, Rauchmeldeanlagen, Feuerlöschgeräte und eine doppelt ausgeführte Klimaanlage zur Verfügung. Der Serverraum wird zusätzlich auf Abweichungen des Raumklimas überwacht.

- Der Datenbestand wird täglich auf Disk-to-Disk gesichert. Datenbestand und Datensicherung sind in getrennten Gebäuden untergebracht. Eine

zusätzliche Sicherung auf Tape findet einmal wöchentlich statt. Diese wird in einem weiteren, verschlossenen Raum untergebracht.

- Es werden anlassbezogene Rücksicherungen durchgeführt, um die Datensicherungsmaßnahmen zu kontrollieren.

IV. Pseudonymisierung und Verschlüsselung

(Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

- Bei der Stadt Weilheim findet keine Pseudonymisierung statt.

V. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Maßnahmen, die die Sicherheit der Verarbeitung gewährleisten.

- Das Datenschutz-Management definiert im laufenden Betrieb kontinuierlich die Verantwortlichkeiten, Strukturen und Prozesse und baut diese im Sinne eines risikobasierten Ansatzes aus. Zur Gewährleistung der Sicherheit der Verarbeitung erstellt die Stadt Weilheim strukturierte Verfahrensbeschreibungen, die im laufenden Betrieb aktualisiert werden.

- Des Weiteren finden regelmäßige Datenschutzschulungen der Mitarbeiter zur erneuten Sensibilisierung statt. Betriebsanweisungen zur Nutzung der Kommunikationssysteme und der IT sind kommuniziert und werden im laufenden Prozess angepasst.

VI. Datenschutzfreundliche Voreinstellungen

(Art. 25 Abs. 2 DSGVO)

Maßnahmen, die grundsätzlich ergriffen werden um den Datenschutz zu gewährleisten.

- Es werden nur diejenigen personenbezogene Daten erhoben, die für den jeweiligen Zweck erforderlich sind.

Stand 06/2020