

Drucksache Nr.: 9543/2020-25

Anfrage zum Datenschutz zur Sitzung des Digitalisierungsausschusses am 27.02.2025

Beantwortung der Anfrage zum Datenschutz:

Mit welchen Maßnahmen stellt die Stadt Bielefeld sicher, dass technischer und organisatorischer Datenschutz in allen städtischen IT-Systemen umgesetzt wird?

Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen der Datenschutz-Grundverordnung (DSGVO) erfüllt werden. Laut Art. 25 DSGVO sind die Maßnahmen zum Schutz der Daten an den Daten selbst, dem Zweck sowie am aktuellen Stand der Technik auszurichten. Es ist daher fortlaufend zu prüfen, ob die getroffenen Maßnahmen zum Schutz der Daten ausreichend oder anzupassen sind. Die Maßnahmen sind nach dem Stand der Technik, den Implementierungskosten und dem Zweck der Datenverarbeitung zu bewerten und ggf. umzusetzen.

Maßnahmen zur Datensicherheit können folglich entweder technischer Natur sein oder sich in organisatorischen Regelungen wie Vorgaben zur Datensparsamkeit, frühzeitigen Anonymisierung oder Pseudonymisierung, aber auch zu Rechten und Rollen ausdrücken. Technische Maßnahmen setzen auf den Einsatz von Technik, regelmäßig über eingesetzte IT-Systeme. Dazu gehören z.B. die Verschlüsselung, Benutzerbeschränkung, Virtualisierung oder Sicherheitskopien. Organisatorische Maßnahmen bestehen etwa aus Dienstanweisungen, der Bestellung von Informationssicherheitsbeauftragten oder Durchführung von Audits.

Zwecks Umsetzung dieser Vorgaben gibt es bei der Stadt Bielefeld mehrere Instrumentarien und Maßnahmen, die den technischen und organisatorischen Datenschutz in städtischen IT-Systemen sicherstellen. Neben der aktuellen Dienstanweisung zum Datenschutz und der Dienstanweisung über die Organisation der Informations- und Datenverarbeitung wurden weitere gesamtstädtische und auch fachbereichsspezifische Dienstanweisungen erlassen, die sich mit Regelungen zum Datenschutz und der Datensicherheit auseinandersetzen. Die Stadt Bielefeld hat sich zudem im Rahmen der erstellten Informationssicherheitsrichtlinie verpflichtet, ein Informationssicherheitsmanagementsystem (ISMS) nach anerkannten Standards (z.B. ISO/IEC 27001 oder BSI-IT-Grundschutz), welches alle rechtlichen Anforderungen erfüllt, aufzubauen. Im Rahmen einer ganzheitlichen Konzeption sorgt dies für einen angemessenen Schutz der IT-Systeme, Anwendungen, Daten und Prozesse und unterstützt, diesen sicherzustellen. In den Regelwerken werden Verantwortlichkeiten und Prozesse festgelegt. Diese stützen Datensicherheit, Datenschutz und somit den Umgang mit personenbezogenen Informationen im Sinne der DSGVO im Rahmen des Projekt- und Prozessmanagements beim Einsatz der städtischen IT-Systeme. Über diese Regelungen wird mindestens ein den normalen Risiken bei der Verarbeitung angemessenes Sicherheitsniveau gewährleistet.

Durch Vorgaben von Bundesbehörden wurde in einigen Bereichen (KFZ-Zulassung: iKfz, Behördennetz des Bundes) ein ISMS dokumentiert, auditiert und zertifiziert. In diesem Rahmen wurden die betroffenen Dienststellen betrachtet, aber auch allgemeine Regelungen für die Gesamtverwaltung. Soweit hier Änderungen erforderlich waren, wurden diese mit Geltung für die Gesamtverwaltung umgesetzt. Die technischen Maßnahmen zur Absicherung der IT sind ebenfalls so konzipiert, dass sie für alle Geräte gelten.

Aktuell wird, gefördert durch die EU, ein ISMS im Gesundheitsamt eingeführt. Die Ergebnisse, soweit sie nicht ohnehin verwaltungsweite Gültigkeit haben, sollen auf andere Ämter übertragen werden.

Beantwortung der Zusatzfrage 1:

Wie wird die konsequente Umsetzung der Prinzipien „Privacy-by-Design“ und „Privacy-by-Default“ erreicht?

Art. 25 DSGVO beschreibt und regelt die beiden Prinzipien Datenschutz durch Technikgestaltung (Privacy-by-Design) sowie durch datenschutzfreundliche Voreinstellungen (Privacy-by-Default) und die Anforderung an die Gestaltung und den Betrieb von Verfahren, die personenbezogene Daten verarbeiten. Auf diese Weise soll der Verantwortliche für die Datenverarbeitung dazu verpflichtet werden, möglichst frühzeitig, also bereits in der Phase des Entwurfs bzw. der Umsetzung eines Verfahrens die Voraussetzungen dafür zu schaffen, dass die Anforderungen der Verordnung, insbesondere die in Art. 5 DSGVO implementierten Grundsätze der Datenverarbeitung, eingehalten werden. Beide Konzepte haben sich zum Ziel gesetzt, die Zweckbindung und Datenminimierung zu optimieren. Sie beziehen sich vor allem auf die Art, den Umfang, die Speicherfristen und die Zugänglichkeit der zu verarbeitenden Daten.

Wie bereits oben zu Frage 1 dargelegt, wurden Maßnahmen und Prozesse implementiert, die sich mit Regelungen zum Datenschutz und der Datensicherheit auseinandersetzen.

Bei der Beschaffung von IT-Systemen, die personenbezogene Daten verarbeiten, wird darauf geachtet, dass diese so gestaltet sind, dass die Datenverarbeitungsgrundsätze beachtet werden. Dies betrifft etwa die Punkte Gestaltung von Eingabefeldern (z. B. Datenminimierung beachten bei Feldkonfiguration als Pflichtfeld, Auswahlliste oder Freitextfeld), unmittelbarer Schutz von personenbezogenen Daten (z. B. Pseudonymisierung, Verschlüsselung), Möglichkeiten zur Datenlöschung und zur Festlegung des Funktionsumfang von Berechtigungskonzepten, Vorgaben zur Festlegung der Notwendigkeit, Passwörter verschlüsselt zu speichern oder den Zugriff auf Daten zu authentifizieren sowie der Möglichkeit, in Softwareprodukten Berechtigungen flexibel zu setzen.

Eine geeignete technische Maßnahme im Rahmen der genannten Prinzipien stellt die Verschlüsselung von Daten beispielsweise bei der Übertragung dar. Eine solche Maßnahme wird durch den Einsatz einer datenschutzkonformen Datenaustauschplattform umgesetzt.

Der in Art. 5 Abs. 1 lit. a) DSGVO genannte Grundsatz der Transparenz wird durch die technische Einbindung von Datenschutzhinweisen auf der Internetseite und der Serviceportal-Seite und den dort angebotenen Onlinediensten umgesetzt.

Der Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c) DSGVO wird durch das Aggregieren von personenbezogenen Daten, beispielsweise bei der Auswertung von Umfragen etc. erreicht.

Die in Art. 5 Abs. 2 DSGVO statuierte Rechenschaftspflicht bedingt die angemessene Dokumentation von Vorgängen, was in technischer Hinsicht z.B. durch (datensparsames) Logging umgesetzt wird. Hierdurch ist als organisatorische Maßnahme beispielsweise durch Erheben von Stichproben anhand der Logging-Daten eine Ahnung von Datenschutzverstößen möglich.

Dem in Art. 5 Abs. 1 lit. c) DSGVO genannten Grundsatz der Zweckbindung wird technisch durch Nutzung eines technisch implementierten Rollen- und Berechtigungskonzepts entsprochen.

Der Speicherbegrenzungsgrundsatz aus Art. 5 Abs. 1 lit. d) DSGVO wird durch in Anwendungen technisch vorgesehene effektive Löschkonzepte und -möglichkeiten erreicht.

Durch den Einsatz von Fachverfahren, die den von der Datenverarbeitung Betroffenen die Wahrnehmung ihrer Betroffenenrechte aus den Artt. 12-23 DSGVO ermöglichen, indem entsprechende Daten extrahiert oder auf Antrag gelöscht werden, werden die Datenverarbeitungsgrundsätze der Transparenz und Datenminimierung sowie Datenbegrenzung umgesetzt.

Im Rahmen der Aufgabenerfüllung der städtischen Fachämter erfolgt eine Verarbeitung in dem Rahmen, der zur Zweckerfüllung notwendig ist. Durch das Rechte- und Rollenkonzept, das über die IT-Systeme umgesetzt wird, ist gewährleistet, dass ein Zugriff lediglich nach dem „Need-to-know-Prinzip“ erfolgt. Auch diese technischen Maßnahmen erfüllen die Anforderung des Datenschutzes durch Technikgestaltung im Sinne von Art. 25 Abs. 1 DSGVO.

Im Rahmen der Aufgabenerfüllung werden Lösch- und Aufbewahrungsfristen festgelegt, so dass der Datenverarbeitungsgrundsatz der Speicherbegrenzung eingehalten wird. Bei der Beschaffung und Implementierung werden in Vergabeverfahren Vorgaben zur Einhaltung datenschutzfreundlicher Voreinstellungen gemacht und Nachweise für deren Umsetzung, beispielsweise durch Vorlage eines Auditberichts oder eines Zertifikats, gemacht. Gleiches gilt für eingesetzte Dienstleister.

Zur Umsetzung der datenschutzfreundlichen Voreinstellungen aus Art. 25 Abs. 2 DSGVO hat die Stadt Bielefeld sicherzustellen, dass grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen Verarbeitungszweck erforderlich ist. Diese Pflicht wird durch Art. 25 Abs. 2 S. 2 weiter konkretisiert, wonach diese Pflicht auch für die Rahmenbedingungen der Verarbeitung wie Art, Umfang, Speicherfrist und Zugänglichkeit gilt. Zwecks Vermeidung von Wiederholungen kann insoweit auf die bereits oben genannten Maßnahmen verwiesen werden.

Die Voreinstellungen von datenschutzrechtlich relevanten Funktionen der Betriebsmittel und anderen Einstellungen der Verarbeitungsmittel sollten so gestaltet sein, dass sie die Grundprinzipien des Datenschutzes und der IT-Sicherheit von vornherein berücksichtigen. Ein Beispiel für die Umsetzung ist die Implementierung der Eingabe von Passwörtern mit der Vorgabe, wie diese zu erstellen sind. Die eingesetzte Hardware ist mit einer Festplattenverschlüsselung versehen. Die Geräte werden zentral administriert und konfiguriert. Es erfolgt die Beschränkung der Berechtigungen von Benutzern, Ortungsdienste werden grds. ausgeschaltet und deren Nutzung aufgabenbezogen geprüft.

Zusammengefasst werden somit folgende Maßnahmen ergriffen:

• Technische und organisatorische Maßnahmen
• Auswahl neuer Software nur von datenschutzkonformen Anbietern und umfangreiche Überprüfung im Vorfeld
• Datenschutzfreundliche Voreinstellungen in der eigenen IT-Infrastruktur
• Nutzung von Produkten und Diensten mit datenschutzfreundlichen Voreinstellungen (z. B. bei Fachanwendungen)
• Löschung von personenbezogenen Daten, wenn diese nicht mehr benötigt werden und der Möglichkeit, dieses in den genutzten Fachanwendungen umzusetzen
• Einbindung des Datenschutzbeauftragten und des Informationssicherheitsbeauftragten vor Einführung eines neuen Verfahrens

Beantwortung der Zusatzfrage 2:

Wie stellt die Stadt sicher, dass städtische Angebote keine Tracker enthalten und dass keine Datenweitergabe zu privaten Anbietern z.B. Facebook ohne explizite Zustimmung stattfindet?

Diese Fragestellung bezieht sich auf den Anwendungsbereich von Art. 25 Abs. 2 DSGVO und den Aspekt der datenschutzfreundlichen Voreinstellungen.

Der Anwendungsbereich von Abs. 2 bezieht sich in erster Linie auf internetbasierte Dienste wie etwa soziale Netzwerke, bei den durch die standardmäßige Konfiguration von Privatsphäre-Einstellungen sicherzustellen ist, dass Nutzer ihre Daten nur den Personenkreisen oder nur dem Umfang zugänglich machen, die sie vorab selbst festgelegt haben. Da beispielsweise die Anmeldung bei Facebook voraussetzt, dass man ein Benutzerkonto erstellt und die Bedingungen von Facebook für die Nutzung akzeptiert und zusätzlich in einer Datenschutzerklärung mitgeteilt wird, in welcher Form die Datenverarbeitung erfolgt, ist die vorherige Zustimmung notwendig, ohne die die Nutzung nicht möglich wäre. Letztlich erfolgt die Nutzung somit auf einer eigenständigen, freiwilligen Entscheidung desjenigen, der sich über ein Facebook-Konto anmeldet. Zusätzlich wird über die Datenschutzerklärung der Stadt Bielefeld den Betroffenen ein transparenter Hinweis erteilt, welche Datenverarbeitungsvorgänge bei der Nutzung von Facebook stattfinden.

Im Übrigen erfolgt beim erstmaligen Aufrufen der Internetseite oder des Serviceportals der Stadt Bielefeld der Hinweis an den Nutzer, dass Cookies und die Analysesoftware Matomo verwendet werden. Insoweit wird darauf hingewiesen, dass eine Einwilligung des Besuchers der Internetseite erforderlich ist, damit die Stadt Bielefeld diese Dienste nutzen kann. Hintergründe werden in einer aufrufbaren Datenschutzerklärung erläutert. Zudem haben die Besucher der Internetseite die Möglichkeit, entsprechende Optionen einzustellen. Folglich ist zunächst ebenso wie bei der Nutzung von Facebook eine Einwilligungserklärung, die vor dem Hintergrund der entsprechenden Hinweise informiert erfolgt, notwendig. Mit dieser Maßnahme werden die Prinzipien des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen umgesetzt.

Der Internetauftritt und die Bielefeld-App werden durch das Presseamt und deren Dienstleister in eigener Verantwortung betrieben und unterliegen wie die sozialen Medien den technisch-organisatorischen Maßnahmen der jeweiligen Betreiber.