Hanse- und Universitätsstadt
Rostock
Die Oberbürgermeisterin

Stellungnahme
2024/AM/5266-01 (SN)
öffentlich

fed. Senator/-in: Oberbürgermeisterin - Grundsatz, Wirtschaft, Ehrenamt und Kultur Federführendes Amt: Büro der Oberbürgermeisterin	Beteiligt: Amt für Digitalisierung und IT Amt für Stadtentwicklung, Stadtplanung und Mobilität

Anfrage von Stephan Porst (Fraktion BÜNDNIS 90/DIE GRÜNEN)

Datenschutzverletzungen

Geplante Beratungsfolge:

Datum	Gremium	Zuständigkeit

Anliegen:

Im Zusammenhang mit der Verarbeitung personenbezogener Daten,
die im Rahmen der Abgabe einer Stellungnahme zu Bauleitplänen erhoben wurden kam es wiederholt zu Datenschutzverstößen durch die Verwaltung der Hanse- und Universitätsstadt Rostock, bei denen personenbezogenen Daten von Personen,
die eine Stellungnahme abgegeben hatten über einen langen Zeitraum völlig ungeschützt bzw. Daten unzureichend anonymisiert öffentlich zugänglich waren.

Bei der Abgabe einer Stellungnahme verpflichtet sich die Hanse- und Universitätsstadt personenbezogenen Daten unter Beachtung nachfolgender Regelungen zu verarbeiten:

„Wenn Sie eine Stellungnahme … einreichen, haben Sie die Möglichkeit, personenbezogene Daten anzugeben. Sie sind nicht verpflichtet, diese Daten anzugeben, und die Eingabe unterliegt ihrer freien Entscheidung. Ihre personenbezogenen Daten werden nur zum Zweck der Verarbeitung Ihrer Stellungnahme verwendet und nicht mit anderen Daten verknüpft oder abgeglichen. Sofern eine Speicherung notwendig ist, um den Zweck der Verarbeitung der Stellungnahme zu erbringen, werden Ihre Angaben auf besonders geschützten Servern nach den Vorgaben der Datenschutzgrundverordnung abgelegt. Eine Speicherung erfolgt für den Zeitraum der Online-Beteiligung und der Auswertung.

Sobald der Speicherungszweck entfällt oder eine durch solche Vorschriften vorgesehene Speicherfrist abläuft, werden die personenbezogenen Daten routinemäßig gesperrt oder gelöscht.“

Dies vorweggeschickt bitte ich um ausführliche und vollständige Beantwortung nachfolgender Fragen: **Hinweis:** Sofern Fragen mit ja/nein/keine o.ä. beantwortet werden, sind zusätzlich erläuternde Angaben beizufügen.

Sachverhalt:

I. Fragenkomplex zum Datenschutzverstoß im Zusammenhang mit der Abgabe einer Stellungnahme:

1. *Die Datenschutzverletzung ist z.T. darauf zurückzuführen dass Daten erhoben wurden, die zur Verarbeitung der Stellungnahme nicht erforderlich waren. So wurde optional die Anschrift erfragt, obwohl keine postalische Zustellung der Abwägung erfolgte. Zu welchem Zweck wurden die freiwillig anzugebenen personenbezogenen Daten genau erhoben?*

Im Rahmen der Auslegung erfolgt die Abfrage nach den Adressdaten. Die Angabe ist freiwillig und zielt darauf ab, das Abwägungsergebnis mitzuteilen. Die Mitteilung erfolgt gemäß BauGB § 3 Absatz 2 Satz 4. Die Mitteilung des Abwägungsergebnisses erfolgt in der Regel zeitverzögert, da die Mitteilung zwar per Gesetz gefordert aber rechtlich für die Wirksamkeit des B-Plans nicht relevant ist. Wenn jemand eine Stellungnahme Anonym abgibt, hat das zur Folge, dass kein Abwägungsergebnis mitgeteilt wird.

2. *Bereits im Jahr 2022 erfolgten Hinweise zu aufgetretenen Datenschutzverletzung:*
   a) Welche Maßnahmen wurden damals infolge der Datenschutzverletzung abgeleitet?

Bis 2022 wurden personenbezogene Daten der einreichenden Bürger*innen geschwärzt und als PDF Datei auf das Portal hochgeladen. Durch eine Manipulation der Datei konnten die personenbezogenen Daten durch Dritte wieder kenntlich gemacht werden. Dieses Vorgehen wurde durch den Landesbeauftragten für Datenschutz und Informationsfreiheit (LfDI) angemahnt und die HRO aufgefordert, die Datenschutzverletzung zu beseitigen. Beim zuständigen Fachbereich wurde daraufhin ein geänderter Prozess eingeführt, der die komplette Anonymisierung der personenbezogenen Daten vorsah. Mittlerweile wird zu der ursprünglichen Datei eine weitere Version erzeugt, die keine personenbezogenen Daten mehr enthält.

Nach der aktuellen Datenschutzverletzung wurde in Abstimmung mit der Abteilung Organisation ein Vier-Augen-Prinzip eingeführt.

b) Erfolgte infolge der Datenschutzverletzung im Jahr 2022 eine Meldung gemäß Art.33 DSGVO?

Eine Meldung der Datenschutzverletzung aus 2022 durch die Stadtverwaltung erfolgte nicht, da der LfDI selbst mit der Meldung der Verletzung auf die HRO zukam. Weitere Datenpannen in diesem Zusammenhang konnten auch nach gründlicher Recherche durch den Fachbereich nicht festgestellt werden.

3. *Im Jahr 2024 kam es erneut zu gleichartigen Datenschutzverletzungen, was systematische Defizite im Zusammenhang mit dem Datenschutz vermuten lässt:*
   a) Warum kam es zur wiederholten gleichartigen Datenschutzverletzung?

Für die Erarbeitung des Bebauungsplanes wurde ein Planungsbüro beauftragt, mit dem zum ersten Mal zusammengearbeitet wurde. Aus diesem Grund war dem Planungsbüro nicht bewusst, dass in Rostock Abwägungstabellen mit Stellungnahmen aus der Öffentlichkeitsbeteiligung grundsätzlich anonymisiert zu erstellen sind. Der Fehler ist im Zuge der Vorbereitung zur Beschlussfassung durch die Bürgerschaft zwar im Amt für Stadtentwicklung, Stadtplanung und Mobilität aufgefallen, sodass eine anonymisierte Fassung erstellt wurde, jedoch ist versehentlich die falsche Fassung der Vorlage angehängt worden.

b) Welche Maßnahmen werden aufgrund des erneuten Vorfalls abgeleitet? - Gab es aufgrund des wiederholten Verstoßes Sanktionen?

Aufgrund der aktuellen Datenschutzverletzung ist angedacht, künftig bereits bei der Beauftragung von Planungsbüros darauf hinzuweisen, dass Unterlagen mit personengebundenen Daten stets in anonymisierter Form aufzubereiten sind. Sanktionen hat es nicht gegeben, da die Datenschutzverletzung nicht aus Vorsatz entstanden ist.

4. *Bei Datenschutzverstößen sind gegebenenfalls betroffenen Personen zu informieren. Ist dies im Fall aller Datenschutzverstöße erfolgt?*

Im Rahmen der aktuellen Datenschutzverletzung ist keine weitere Person betroffen. Betroffene von früheren Datenschutzverletzungen werden entsprechend den Anforderungen aus Art. 34 DSG-VO informiert.

5. *Erhobene personenbezogenen Daten werden gemäß Datenschutzhinweisen auf besonders geschützten Servern abgelegt.*
   a) Wodurch ist ein besonders geschützter Server im Unterschied zu normalen Dateiservern der Verwaltung gekennzeichnet?
   b) Wie ist der Zugang zu diesen Servern geregelt?
   c) Ist der, das KSD hostende Server ein besonders geschützter Server?

Unter Hinweise zum Datenschutz der Verfahrensträger Amt für Stadtentwicklung, Stadtplanung und Mobilität heißt es:

„3. Umgang mit personenbezogenen Daten

Wenn Sie eine Stellungnahme im Rahmen eines vom Verfahrensträger durchgeführten Beteiligungsverfahrens einreichen, haben Sie die Möglichkeit, personenbezogene Daten anzugeben. Sie sind nicht verpflichtet, diese Daten anzugeben, und die Eingabe unterliegt ihrer freien Entscheidung. Ihre personenbezogenen Daten werden nur zum Zweck der Verarbeitung Ihrer Stellungnahme verwendet und nicht mit anderen Daten verknüpft oder abgeglichen. Sofern eine Speicherung notwendig ist, um den Zweck der Verarbeitung der Stellungnahme zu erbringen, werden Ihre Angaben auf besonders geschützten Servern nach den Vorgaben der Datenschutzgrundverordnung abgelegt. Eine Speicherung erfolgt für den Zeitraum der Online-Beteiligung und der Auswertung.“

Diese Server sind durch technische und organisatorische Maßnahmen gegen Verlust, Zerstörung, Zugriff, Veränderung oder Verbreitung Ihrer Daten durch unbefugte Personen geschützt. Der Zugriff auf ihre Daten ist nur wenigen, befugten Personen möglich. Der Personenkreis ist auf den mit dem Bauleitplanverfahren befassten Personenkreis beschränkt. Trotz aller möglichen Sicherheitsmaßnahmen ist ein vollständiger Schutz gegen alle Gefahren jedoch nicht möglich.

Im vorliegenden Fall werden verschiedene Server, die nicht miteinander kommunizieren können, als Einheit dargestellt. Eine automatische Datenübernahme vom Bauleitplanserver auf den ALLRIS-Server kann nicht erfolgen.

Die Ergebnisse der Öffentlichkeitsbeteiligung werden in einer gesonderten Tabelle zusammengestellt und in der Abwägung verarbeitet. Die Abwägung ist zentraler Punkt eines Satzungsbeschlusses für einen Bebauungsplan und als Anlage zum Beschluss in der ALLRIS-Vorlage eingestellt. Die Übernahme ins ALLRIS erfolgt manuell als PDF und stellt hier die Fehlerquelle dar, da einmal die Schwärzung der Personendaten nicht irreversibel erfolgt und beim zweiten Mal die falsche Datei angehängt worden ist.

Alle Server der Stadtverwaltung sind besonders geschützte Server.

Die in ALLRIS gehaltenen Daten werden über einen Applikationsserver gespeichert und verwaltet, dabei handelt es sich nicht um einen "normalen Fileserver".

Es gibt für die Nutzenden keinen direkten Zugriff auf die Daten/ Dateien, nur den Zugriff über die Applikation bzw. den Webclient. In einem Berechtigungskonzept werden die Zugriffe zu nichtöffentlichen Vorlagen und gesondert zu Personalvorlagen geregelt. Zugriff zu den Personenstammdaten der Gremienmitglieder haben nur die mit der Pflege dieser Daten beauftragten Mitarbeiter.

6. *Existieren besondere Verhaltensregeln/ Datenschutzkonzepte im Amt für Stadtentwicklung, Stadtplanung und Mobilität für die Verarbeitung personenbezogenen Daten, die im Zusammenhang mit abgegebenen Stellungnahmen erhoben wurden?*

Wie bereits zur Frage 3a erläutert wurde, sind alle Stellungnahmen, die im Zuge einer Öffentlichkeitsbeteiligung gemäß § 3 Abs. 1 und § 4 Abs. 1 BauGB abgegeben wurden, in einer anonymisierten Tabelle darzustellen und so der Bürgerschaft zur Beschlussfassung vorzulegen.

7. *Gab es Prüfungen, ob im KSD weitere Stellungnahmen existieren, in denen personenbezogene Daten unberechtigt veröffentlicht wurden? Wenn ja, wurden weitere Verstöße festgestellt?*

Es wurden alle Abwägungsdokumente im KSD geprüft, welche in der aktuellen Legislaturperiode der Bürgerschaft eingestellt wurden. Dabei sind weitere Datenschutzverletzungen ermittelt worden. Die Betroffenen werden informiert und die Verstöße behoben. Eine Meldung der Datenschutzverstöße an den LfDI erfolgt durch die Datenschutzbeauftragte.

II. Fragenkomplex zum Datenschutz allgemein

1. *Meldungen zum Datenschutz*
   a) Wie viele Datenschutzverletzungen/Datenschutzverstöße durch die Verwaltung der Hanse- und Universitätsstadt Rostock gab es im Zeitraum 2019-2024?

Im Zeitraum zwischen 2019 und 2024 wurden der behördlichen Datenschutzbeauftragten 17 Datenpannen angezeigt. Das Ausmaß der Datenschutzverletzungen und der Eingriffe in die Rechte des einzelnen Betroffenen variierten dabei stark. In der überwiegenden Anzahl der Fälle ließen sich die Pannen ohne erheblichen Aufwand kurzfristig beseitigen und ein Schaden für die Betroffen entstand nicht.

b) Gab es dabei spezielle Häufungen in einzelnen Amtsbereichen?

Eine Häufung konnte nicht festgestellt werden.

c) Gab es Datenschutzverstöße, die als gravierend einzustufen sind?

Es gab bisher eine Datenschutzverletzung, bei der der Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) derzeit Auflagen prüft (aktueller Phishing-Angriff aus dem Februar), welche der HRO auferlegt werden könnten um den Datenschutz zu verbessern. Bei allen anderen Datenschutzverletzungen ist die Aufsichtsbehörde zu dem Schluss gekommen, dass keine Verwarnung oder gesonderte Auflagen von Nöten sind, da die HRO den datenschutzrechtlichen Anforderungen gerecht wird.

d) Welche wesentlichen Maßnahmen wurden aus etwaigen Datenschutzverstößen abgeleitet?

Intern wird bei jeder Datenschutzverletzung in Zusammenarbeit mit dem Amt für Digitalisierung und IT und der Abteilung Organisation des Hauptamtes geprüft, ob technische oder arbeitsorganisatorische Maßnahmen ergriffen werden, welche den Schutz der personenbezogenen Maßnahmen verbessert. Dabei kann sich beispielsweise der Bedarf ergeben, eine zusätzliche Datenschutzschulung durchzuführen, eine Vier-Augen-Kontrolle einzuführen oder die technischen Rechte- und Rollenkonzepte zu überarbeiten.

2. *Datenschutzkonzept:*
   a) Gibt es ein Datenschutzkonzept? Wann wurde dies letztmalig aktualisiert?

In der Verwaltung der HRO gibt es eine Geschäftsanweisung zum Datenschutz sowie die sogenannten Verzeichnisse der Verarbeitungstätigkeit für jede Verarbeitungstätigkeit der HRO. Die Geschäftsanweisung regelt die Verantwortlichkeiten und beschreibt die datenschutzrechtlichen Anforderungen zur Verarbeitung von personenbezogenen Daten innerhalb der HRO, während die Verzeichnisse für jede Verarbeitungstätigkeit die konkreten Rechtgrundlagen, Empfänger, Speicherorte, Aufbewahrungsfristen, sowie die getroffenen technisch-organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten für diese Verarbeitungstätigkeit dokumentieren.

Die Geschäftsanweisung zum Datenschutz wurde letztmalig im November 2023 aktualisiert. Die Verfahrensverzeichnisse werden bei Änderungen im Verfahren angepasst.

b) Gibt es ein Löschkonzept für personenbezogenen Daten?

Die Aufbewahrungsfristen werden in den Verzeichnissen zu den einzelnen Verarbeitungstätigkeiten dokumentiert. Diese richten sich nach den gesetzlich festgelegten Aufbewahrungsfristen. Die regelmäßige Archivierung bzw. Löschung der papiergebundenen Unterlagen, sowie der Dateien auf den Laufwerken obliegt den Ämtern. Für übergreifende Software wie beispielweise das Dokumentenmanagementsystem d.3 gibt es zentrale Löschkonzepte, die eine automatisierte Löschung bzw. Archivierung der Akten nach Vorgabe der Ämter vorsehen.

c) Wurden die Einhaltung der Datenschutzbestimmungen und das Datenschutzkonzept jemals auditiert?

Es gab bisher keine Auditierung durch einen externen Dienstleister oder die Aufsichtsbehörde. Im Rahmen der Aktualisierung der Dokumentationen und bei Datenpannen wurden bereichsweise Räumlichkeiten (Zutrittsbeschränkungen), Rechte- und Rollenkonzepte (Zugriffrechte) durch die behördliche Datenschutzbeauftragte geprüft sowie bereichsspezifische Schulungen durchgeführt.

d) Wie und wie regelmäßig erfolgt verwaltungsintern die Überwachung auf Einhaltung der Datenschutzbestimmungen?

Siehe c) Die Umsetzung der datenschutzrechtlichen Anforderungen obliegt gemäß Geschäftsanweisung zum Datenschutz den Ämtern der Stadtverwaltung. Diese nutzen die Beratungsleitung der behördlichen Datenschutzbeauftragten und tragen dafür Sorge, dass die Verarbeitung von personenbezogenen Daten datenschutzkonform erfolgt. Die Datenschutzbeauftragte wird daher bei Anpassungen in Verfahrensabläufen einbezogen, bei der Neuanschaffung/ Vergabe von Software und Dienstleistungen, bei Digitalisierungsprozessen, sowie zur Prüfung von internen Geschäftsanweisungen, Dienstvereinbarungen und der Erfüllung von Betroffenenrechten.

3. *Schulungen zum Datenschutz:*
   a) Existiert eine regelmäßige Pflichtschulung aller Mitarbeiter zum Datenschutz und dem Umgang mit Datenschutzverstößen?
   b) Wie regelmäßig erfolgt die Schulung und wie wird dies dokumentiert?
   c) Beinhalten die Schulungen eine Erfolgskontrolle?

Die Geschäftsanweisung zum Datenschutz regelt, dass alle Mitarbeitenden einmal jährlich, aktenkundig zum Datenschutz belehrt werden müssen. Dazu stellt die behördliche Datenschutzbeauftragte ein Belehrungsformular sowie ein dreiseitiges Infoblatt zur Verfügung. Dem Infoblatt lassen sich die Grundsätze für die datenschutzkonforme Verarbeitung sowie die Pflichten zur Wahrung der Betroffenenrechte entnehmen. Jeder Mitarbeitende muss bestätigen, dass er die Informationen gelesen hat und verpflichtet sich den datenschutzrechtlichen Anforderungen im Rahmen seiner Tätigkeit bei der HRO nachzukommen.

Zusätzlich wurde durch die Datenschutzbeauftragte im letzten Jahr ein digitales E-Learning zum Datenschutz aufgebaut, welches jedem Mitarbeitenden über die Plattform der VHS-Cloud zur Verfügung steht. Bisher wurde eine Teilnahme am E-Learning in Eigeninitiative der Mitarbeitenden oder auf Anordnung der Führungskräfte durchgeführt. Sollte die Führungskraft die Schulung angeordnet haben, erfolgt eine Rückmeldung durch die behördliche Datenschutzbeauftragte, ob alle Mitarbeitenden den Kurs absolviert haben. Im Personalqualifizierungsprogramm der HRO werden jährlich zwei Datenschutzschulungen sowie bereichsspezifische Schulungen in Persona angeboten.

Auch die Teilnahme an den persönlichen Schulungsangeboten wird üblicherweise durch die Führungskräfte angeordnet, es steht aber grundsätzlich auch jedem interessierten Mitarbeitenden frei, sich anzumelden.

Darüber hinaus wird aktuell in Zusammenarbeit mit dem Amt für Digitalisierung und IT ein Awareness-Plan in Bezug auf Phishing-Angriffe und IT-Sicherheit erarbeitet.

Finanzielle Auswirkungen:

keine

Eva-Maria Kröger

Anlagen
Keine