► Nr. VO/2022/10854
öffentlich

Lübeck, 14.02.2022

Anfrage

Bearbeitung: Joanna Kjer (E-Mail: joanna.kjer@luebeck.de Telefon: 122-1070)

Anfrage des AM Lars Lehrke (Die Unabhängigen) und Birte Duggen (Bündnis90/Die Grünen): Verkauf von Datenträger mit personenbezogenen Daten der Hansestadt auf Ebay

Beratungsfolge:

Datum	Gremium	Status	Zuständigkeit
22.02.2022	Hauptausschuss	Öffentlich	zur Kenntnisnahme

Anfrage:
In der Sitzung des Hauptausschusses am 08.02.2022 wurde im nicht-öffentlichen Bereich über die publik gewordene Datenschutzpanne berichtet und erste Fragen hierzu beantwortet. Nachstehende weitere Fragen ergeben sich aus den Ausführungen der Verwaltung und mögen bitten in der nächsten Sitzung des Hauptausschusses beantwortet werden.

1) Welche Standards und Regularien zum Schutz personenbezogener Daten existierten in der Lübecker Verwaltung zum Zeitpunkt des Verkaufs von Datenträgern mit personenbezogenen Daten auf Ebay?
    a. Existierten technische Vorkehrungen, die das Ablegen unverschlüsselter und nicht passwortgeschützter Dateien mit personenbezogenen Daten unterbinden?
    b. Wurde ggf. stichprobenhaft geprüft, ob Mitarbeiter:innen unverschlüsselte und nicht passwortgeschützte Dateien mit personenbezogenen Daten auf lokalen Speichermedien ablegen? Wenn ja, wie häufig und wie häufig wurden solche Dateien entdeckt?
    c. Existierten Dienstanweisungen, die das Ablegen unverschlüsselter und nicht passwortgeschützter Dateien mit personenbezogenen Daten auf lokalen Speichermedien untersagen?
    d. Wenn ja, wie und wie häufig wurden die Mitarbeiter:innen zu den Inhalten dieser Dienstanweisung geschult? Und wie und wann wurden neue Mitarbeiter:innen über die Inhalte dieser Dienstanweisung unterrichtet?
    e. Welche Löschvorgänge wurden standardmäßig unternommen bei Übergabe eines personalisierten Rechners an andere Mitarbeitende?
    f. Welche Datenverarbeitungsvorgänge sind hierzu im Verzeichnis für Verarbeitungstätigkeiten aufgeführt (insbesondere Löschfristen, Schutzmaßnahmen zur Datensicherheit usw.)
    g. Existierten sonstige technisch organisatorische Maßnahmen, um die Pseudonymisierung und Verschlüsselung personenbezogener Daten gemäß Art. 32 Abs. 1 DSGVO zu gewährleisten?
    h. Welche gemäß DSGVO verpflichtende Dokumentation liegt vor über die ergriffenen technisch organisatorischen Maßnahmen zum Schutz personenbezogener Daten?
2) Nachdem die Vorgänge, die zur Datenschutzpanne führten, untersucht wurden, welche weiteren internen Maßnahmen werden ergriffen, um die Gefahr einer Wiederholung eines solchen Vorfalls zu reduzieren?

a. Verhinderung des Ablegens unverschlüsselter und nicht passwort-geschützter Dateien auf lokalen Speichermedien mit personenbezogenen Daten durch:
    i. Technische Vorkehrungen
    ii. Organisatorische Vorkehrungen (Aufnahme entsprechender Regelungen in die Dienstanweisung IT)
    iii. Kommunikation und ggf. Schulung/ Einweisung der Mitarbeitenden in diese Regelungen
    iv. Gesonderte Löschvorgänge, insbesondere bei Übergabe eines personalisierten Rechners an andere Mitarbeitende
b. Einführung des Vier-Augen-Prinzips beim Ausbau zu entsorgender Datenträger (Festplatten)
c. Höhere Mindeststandards bei der Auswahl der Dienstleister, die Zugang zu personenbezogenen Daten haben.
d. Einführung sonstiger technisch organisatorischer Maßnahmen, um die Pseudonymisierung und Verschlüsselung personenbezogener Daten gemäß Art. 32 Abs. 1 DSGVO zu gewährleisten?

Begründung:
Der bisherigen Berichterstattung war zu entnehmen, dass die Panne im Wesentlichen auf das Verschulden Dritter zurückgeführt wird und diese Gefahr durch eine sorgfältigere Auswahl eines neuen Dienstleisters behoben werden soll. Über etwaige interne Vorkehrungen, die darüber hinaus im Zuge der Erkenntnisse neu zu treffen wären, wurden bislang keine Aussagen getätigt.

Anlagen: