ULD

www.datenschutzzentrum.de

Landesbeauftragte für Datenschutz · Postfach 71 16 · 24171 Kiel

Christina Franke
[redacted]

Landesbeauftragte für Datenschutz
Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223
Ansprechpartner/in:
[redacted]
Durchwahl: 988-[redacted]

Aktenzeichen:
LD3-50.01/22.004

Kiel, 29.06.2022

Ihre Beschwerde vom 21.12.2021

Sehr geehrte Frau Franke,

vielen Dank für Ihre Anfrage vom 21.11.2021 und Ihre Ergänzung vom 21.12.2021 auf die Antwort des ULD vom 20.12.2021. Leider hat sich die Beantwortung verzögert. Ihre Beschwerde wird außerhalb des Portals für Informationsfreiheit („FragdenStaat") und unter einem neuen Aktenzeichen bearbeitet. Wenn Sie uns eine E-Mail-Adresse zusenden, können wir künftig auch darüber kommunizieren.

Zusammengefasst ergeben sich Ihrer E-Mail vom 21.11.2021 und den dort angesprochenen Punkten aus „https://fragdenstaat.de/anfrage/verschlusselung-un-sicherheit-der-verwaltungportale" folgenden Beschwerdepunkte für das Verwaltungsportal „https://serviceportal.schleswig-holstein.de/Verwaltungsportal/" in Schleswig-Holstein:

1. eine hohe Wahrscheinlichkeit für „das Fehlen einer Verschlüsselung" ;
2. eine abweichende Domänenbezeichung zwischen Portal und gesendeten E-Mails;
3. die Tatsache, dass ein Postfach automatisch und somit aus Sicht der Beschwerdeführerin verpflichtend eingerichtet wird;
4. in den Datenschutzerklärungen: kein Verweis auf Artikel 6 Abs. 1 Buchstabe c DSGVO (nach Ihrer Ansicht einschlägig), stattdessen an einer Stelle ein Verweis auf Artikel 6 Abs. 1 Buchstabe f DSGVO;
5. Bitte um Überprüfung, ob Verträge gemäß Artikel 28 DSGVO vorliegen; dazu ein Verweis auf eine weitere Anfrage bei Frag den Staat („https://fragdenstaat.de/anfrage/?user=v.maier_3").

Zu 1) Eine Transportverschlüsselung der Kommunikation zwischen Browser der Nutzenden und Server des Serviceportals ist ersichtlich implementiert. Dass weitergehende Verschlüsselungsmaßnahmen im Rahmen der Implementierung des Serviceportals und seiner Funktionen als technisch-organisatorische Sicherheitsmaßnahmen gefordert sind, geht aus den Regelungen des Artikel 32 Abs. 1 DSGVO nicht hervor: Artikel 32 Abs. 1 Buchstabe a) DSGVO fordert nicht ausnahmelos den Einsatz

von Verschlüsselung, sondern nennt in der Aufzählung a) – d) beispielhafte Maßnahmen, Fähigkeiten und Verfahren, um die Zielsetzungen des Artikel 32 DSGVO zu erreichen. Die Tatsache der beispielhaften Aufzählung wird aus der deutschen Sprachfassung der DSGVO möglicherweise nicht deutlich; aus der englischen Sprachfassung geht dies klar hervor „ the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: ….". Daher wird in der Kommentarliteratur zur DSGVO darauf verwiesen, dass es im Ermessen des Verantwortlichen bzw. des Auftragsverarbeiters steht, wie die Ziele des Artikel 32 DSGVO unter Berücksichtigung der in der Aufzählung genannten Regelbeispiele umgesetzt werden.

Dies wäre anders, wenn spezifische gesetzliche Regelungen oder behördliche Vorgaben, etwa aus Anschlussbedingungen für spezielle Fachverfahren, einschlägig wären. Solche sind hier nicht bekannt. Zum gegenwärtigen Informationsstand ist keine Datenschutzverletzung erkennbar.

Zu 2) Dies wurde für die Tätigkeiten „Kontoregistrierung" und „Passwortrücksetzung" überprüft. Wie von Ihnen dargestellt, erfolgt die Kommunikation über verschiedene Domains: die webbasierte Kommunikation des Serviceportals nutzt die Domain „serviceportal.schleswig-holstein.de" (URL „https://serviceportal.schleswig-holstein.de"), die Versendung der E-Mails aus dem Serviceportal erfolgt durch die E-Mail-Adresse „nonreply-serviceportal-schleswig-hostein@dataport.de."

Bewertung:
Die E-Mail-Domäne der Landesregierung Schleswig-Holstein lautet „landsh.de"; E-Mail-Adressen sind nach dem Muster „<Name>@<Behördenname>.landsh.de" aufgebaut.
Webauftritte von Behörden werden überwiegend im zentralen Portal www.schleswig-holstein.de bereitgestellt, daneben gibt es weitere Websites nachgeordneter Behörden und anderer öffentlicher Stellen (z. B. Landtag , Landesrechnungshof). Insofern fallen E-Mail-Adressen und Domains der Webauftritte von Landesbehörden in den meisten Fällen auseinander; über die Domain schleswig-holstein.de erfolgt keine E-Mailkommunikation.

Im hier zu bewertenden Fall ist die Unterscheidung zwischen der Serviceportaldomain und der vom Dienstleister Dataport zum E-Mail-Versand verwendeten Domain nicht optimal. E-Mails sind aber im Hinblick auf die Absenderadressierung dem Portal zuzuordnen. Einen datenschutzrechtlichen Verstoß gegen Artikel 25 und 32 DSGVO stellt dies nicht dar. Da dies dennoch Fragen bei den Nutzenden aufwerfen kann und diese eine Phishingverdacht hegen könnten, werden wir einen Hinweis an das zuständige Ministerium formulieren, dass im Registrierungsprozess an prominenter Stelle auf die verwendeten E-Mail-Adressen hingewiesen werden sollte.

Zu 3) Laut Darstellung der Datenschutzerklärung wird ein Postfach automatisch eingerichtet. Dies monieren Sie im Hinblick auf § 2 Abs. 7 OZG. Dieser lautet: „(7) Ein „Postfach" ist eine IT-Komponente, über die eine Behörde Nutzern mit deren Zustimmung elektronische Dokumente und Informationen bereitstellen kann. Das Postfach ist Bestandteil eines Nutzerkontos. Die Nutzung eines Postfachs ist für die Nutzer freiwillig."

Bewertung:
§ 2 Abs. 7 Satz 2 OZG kann so interpretiert werden, dass bei der (gemäß § 2 Abs. 6 Satz 5 OZG freiwilligen) Verwendung eines Nutzerkontos stets ein Postfach eingerichtet wird („Das Postfach ist Bestandteil eines Nutzerkontos"), die Nutzung hingegen freiwillig erfolgt („Die Nutzung eines Postfachs ist für die Nutzer freiwillig.", § 2 Abs. 7 Satz 3 OZG). In Artikel 9 Abs. 1 Satz OZG wird ebenfalls auf die Einwilligung abgestellt, die erforderlich dafür ist, dass elektronische Verwaltungsakte durch Abruf aus dem Postfach bekannt gegeben werden können.

Eine datenschutzrechtliche Beschwer ist durch die reine Bereitstellung eines Postfachs nicht erkennbar; ähnlich hat sich auch der BfDI im Schreiben vom 16.11.2021 an Sie geäußert. Dies wäre anders,

wenn ohne Einwilligung elektronische Verwaltungsakte im Postfach abgelegt würden. Dafür bestehen derzeit keine Anhaltspunkte.

Zu 4) Die Datenschutzerklärung unterscheidet zwei Fälle:

a) Verarbeitung bei rein informatorischen Besuchen der Webseite
b) Verarbeitung bei Registrierung

Im Fall a) werden die typischen Daten eines Browsersabrufs (IP-Adresse, Zeit, Zeitzone, abgerufene Seite, Statuscode, übertragene Datenmenge, Ursprungswebseite der Anforderung) sowie die typischerweise vom Browser übertragenen Daten (Browser, Betriebssystem, Sprache, Version) genannt und die Datenübertragung auf Artikel 6 Abs. 1 Buchstabe f DSGVO gestützt. Als Zweck wird die Bereitstellung der Information, Stabilität und Sicherheit genannt.

Im Fall b) werden Stammdaten der Konten in den Ausprägungen „Servicekonto" und „Servicekonto Plus" verarbeitet, die katalogartig genannt sind; zusätzlich das „Datum der Einwilligung zur Datenverarbeitung". Als Rechtsgrundlagen werden § 8 OZG i.V.m. § 1 ZStBaDiVO und §3 Abs. 1 LDSG SH genannt.

Bewertung:

Die Darstellung von Informationen dürfte sich bei behördlicher Tätigkeit auf Artikel 6 Abs. 1 Buchstabe e in Verbindung mit der Umsetzung des OZG stützen lassen. Ob darüber hinaus Behörden Aspekte der Datenverarbeitung (z. B. Stabilität der Webseite, Sicherheit) auf die Generalklausel des Artikel 6 Abs. 1 Buchstabe f DSGVO stützen können, ist strittig; sie ließen sich jedoch alternativ auf Artikel 6 Abs. 1 Buchstabe e DSGVO (Stabilität) und Artikel 6 Abs.1 Buchstabe c DSGVO (Sicherheit) stützen, so dass sich die Anforderung der Rechtmäßigkeit erfüllen lässt.

Die für den Fall (b) genannten Rechtsgrundlagen sind nachvollziehbar und werden von Ihnen nicht moniert. Missverständlich ist aber im Registrierungsprozess die Verwendung des Wortes „Einwilligung": Zum einen ist die Erteilung einer „Einwilligung" als notwendig zu aktivierende Checkbox ausgebildet ist, zum anderen wird das „Datum der Einwilligung" als Stammdatum gespeichert.

Die Eröffnung eines Nutzerkontos (das „Ob") beruht zwar auf einer Entscheidung der Nutzenden, stützt sich aber inhaltlich nicht auf eine Einwilligung gemäß Artikel 6 Abs. 1 Buchstabe a DSGVO, sondern, wie auch in der Datenschutzerklärung dargestellt, auf § 8 OZG i.V.m. § 1 ZStBaDiVO und § 3 Abs. 1 LDSG SH.

Aus hiesiger Sicht ist dies nicht zu beanstanden; an das zuständige Ministerium werden wir jedoch einen Hinweis formulieren, die missverständliche Bezeichnung als „Einwilligung" anzupassen.

Zu 5) Die vertraglichen Regelungen zwischen dem Dienstleister Dataport und dem zuständigen Ministerium waren Gegenstand eines Vermittlungsverfahrens des ULD zwischen dem Ministerium und einer anfragenden Person. Dabei ging es um den Umfang der vertraglichen Regelungen sowie Kosten für eine notwendige Schwärzung in Vertragsanlagen.

Die in diesem Rahmen von Ministerium dargestellte Vertragsstruktur (EVBIT-Verträge, Einbindung Allgemeiner Geschäftsbedingungen, Spezifizierung des Vertragsgegenstand und vertragliche Einbeziehung von Sicherheitskonzepten sowie weiterer Dokumente in Anlagen) wird typischerweise verwendet. Dabei werden zum einen verfahrensspezifische Aspekte geregelt, zum anderen wird auf verfahrensübergreifende Sicherheitsaspekte (etwa zur baulichen Sicherheit von Rechenzentren), die in zahlreichen Verfahren relevant sind, Bezug genommen.

Daher bestehen hier keine grundsätzlichen Zweifel am Vorliegen einer vertraglichen Regelung gemäß Artikel 28 DGSVO. Wir nehmen aber Ihre Anfrage als Prüfhinweis auf und werden in diesem Zusammenhang insbesondere die Vertragsstruktur betrachten, ob alle Aspekte des Artikel 28 DSGVO abgedeckt sind.

Mit freundlichen Grüßen
Im Auftrag

gez. [redacted]