

Per E-Mail:

██████████

Ihr Zeichen: #226637

Ihre Nachricht vom: 01.09.2021

Mein Zeichen: V 30 - 20345/2021

Meine Nachricht vom: 30.08.2021

28. Okt. 2021

Sicherheit des Bürgerportals [#226637]

Sehr geehrte ██████████,

bezugnehmend auf Ihren Antrag auf Informationszugang vom 11.08.2021 über Frag-den-Staat, der hiesigen Antwort an Sie vom 31.08.2021 und der damit gemäß § 4 Abs. 2 IZG SH verbundenen Bitte um Präzisierung Ihres Antrages und Ihres sich daraus ergebenden Schreibens vom 01.09.2021 erteile ich Ihnen gemäß §§ 3, 6 IZG SH folgende Auskunft:

1. Die zur Umsetzung des Onlinezugangsgesetzes (OZG) erforderliche digitale Infrastruktur, über die der gemäß § 1 OZG zu gewährleistende Portalverbund und die Zurverfügungstellung der digitalen Verwaltungsleistungen durch Schleswig-Holstein realisiert werden, setzt sich aus einer im Auftrag des Landes durch den IT-Dienstleister Dataport entwickelten und betriebenen Plattform sowie entsprechender Plattform- und Onlinediensten zusammen. Diese Mehrheit an IT-Komponenten und Lösungen, die sogenannte Online-Service-Infrastruktur (OSI) wird in Kooperation zwischen Schleswig-Holstein und weiteren Bundesländern, den Dataport-Trägerländern, entwickelt, weiterentwickelt und betrieben (siehe dazu auch <https://www.dataport.de/was-wir-bewegen/portfolio/osi/>).

Die Plattform dient als Grundlage für verschiedene E-Government Basisdienste zu denen u.a. das Nutzerkonto gemäß § 2 Abs. 5 OZG zählt. Den Zugang zu diesem und den weiteren digitalen Angeboten erhalten Sie über die Portalseite <https://serviceportal.schleswig-holstein.de/Verwaltungsportal/>.

Aufgrund der Präzisierung Ihres Antrages teile ich Ihnen mit, dass Grundlage der Beauftragung des Betriebs und die damit verbundene Datenverarbeitung ein

geschlossener Betriebsvertrag zwischen dem Land Schleswig-Holstein und Dataport ist (V15183). Dieser wird jährlich in entsprechenden Vertragsreviews den aktuellen Bedingungen angepasst. In entsprechenden Gremien, wie u.a. dem regelmäßig mindestens monatlich tagenden OSI-Board, steuert und kontrolliert Schleswig-Holstein zusammen mit den anderen Auftraggebern die Weiterentwicklung und den Betrieb der Plattform und der Dienste.

Teil dieses Betriebsvertrages sind Service-Level-Agreements in der Details über Art und Umfang der Datenverarbeitung sowie die entsprechenden technischen und organisatorischen Maßnahmen der IT-Sicherheit vereinbart wurden.

Gegenstand der Anlage 5 - „Leistungsbeschreibung - Service Level Agreement OSI Betrieb - Spezifischer Teil für die Produktionsumgebung“ sind Regelungen zu den folgenden Themen:

SLA: Allgemeines, Betriebszeit, Supportzeit, Leistung(Verfügbarkeit), Eskalation
Leistungsreport

SLA-Nr. FM-01: Servicekonto Dienstleistungsbeschreibung, Leistung (Verfügbarkeit, Performance, Produkte), Leistungsreport

SLA-Nr. FM- 02:Postfach Dienstleistungsbeschreibung, Leistung (Verfügbarkeit, Performance, Produkte), Leistungsreport

SLA-Nr. FM-03.02: Service Connector, Dienstleistungsbeschreibung, Leistung (Verfügbarkeit), Leistungsreport

SLA-Nr. FM-05: LoadServer, Dienstleistungsbeschreibung, Leistung (Verfügbarkeit, Performance, Produkte), Leistungsreport

SLA-Nr. FM-06: GMM Connector, Dienstleistungsbeschreibung, Leistung (Verfügbarkeit, Performance, Produkte), Leistungsreport

SLA-Nr. FM-07: Integrator (API-Gateway), Dienstleistungsbeschreibung, Leistung (Verfügbarkeit, Performance, Produkte), Leistungsreport

SLA-Nr. FM-08: E-Payment Dienstleistungsbeschreibung, Leistung (Verfügbarkeit, Performance, Produkte), Leistungsreport

Teil des Vertrages ist außerdem ein weiteres Service-Level-Agreement, Anlage 8b „Zusätzliche Maßnahmen für den grundschutzkonformen Betrieb der Online-Service-Infrastruktur Plattform (OSI) - Verfahrensspezifischer Teil (Teil B)“, in dem folgende zusätzliche Sicherheitsmaßnahmen geregelt sind: Maßnahmen zur Systemüberwachung, Systemlastmessung und Alarmierung, Erarbeitung einer sicheren Verfahrensarchitektur, Verschlüsselung der Datenübermittlung, Tier-System, Erstellung und Umsetzung eines Redundanzkonzeptes, Verifikation von Nutzereingaben, Test- und Deployment Konzept, AV-Konzept und Authentifizierungskonzept.

Zugleich enthält der Vertrag die folgende konkretisierenden Angaben bezogen auf die Auftragsverarbeitung personenbezogener Daten.

Selbstauskunft Auftraggeber über Auftragsverarbeitung

Angaben zum Vertrag über Auftragsverarbeitung

Für die Verarbeitung der in Rede stehenden personenbezogenen Daten gelten folgende Datenschutzregelungen:	Zutreffendes ankreuzen
Verordnung (EU) 2016/679 (DSGVO) und gfls. ergänzende landesrechtliche Regelungen	<input checked="" type="checkbox"/>
Nationale Regelungen (Landesdatenschutzgesetz bzw. Bundesdatenschutzgesetz) zur Umsetzung der RiLi (EU) 2016/680 (Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit)	<input type="checkbox"/>
Es findet keine Verarbeitung personenbezogener Daten statt	<input type="checkbox"/>

Angaben zum Gegenstand der Auftragsverarbeitung¹

Eine Erläuterung zu den nachfolgend zu machenden Angaben findet sich z. B. hier:
https://www.lida.bayern.de/media/dsk_hinweise_vov.pdf

1. Art und Zweck der Verarbeitung (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO)	<ul style="list-style-type: none"> - Servicekonten für Bürger und Unternehmen / Behörden für Online-Dienste - elektronische Kommunikation auf Basis von Servicekonto-Postfächern im Kontext von Online-Dienstleistungen
2. Beschreibung der Kategorien von personenbezogenen Daten (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO bzw. Art. 30 Abs. 1 S. 2 lit. c)	<ul style="list-style-type: none"> - Kundendaten (Vor- und Nachname, E-Mail-Adresse, Postanschrift (Straße, Hausnummer, PLZ, Ort, Land), Geburtsdatum, Servicekontotyp, Datum der Einwilligung zur Datenverarbeitung) - Organisationsdaten (Name der Organisation, Anschrift (Straße, Hausnummer, PLZ, Ort, Land), freigeschaltete Online-Dienste) - Postfachnachrichten (verfahrensabhängig) <p>darunter Kategorien besonderer personenbezogener Daten (siehe z. B. Art. 9 Abs.1 DSGVO)</p>
3. Beschreibung der Kategorien betroffener Personen (siehe z. B. Art. 28 Abs. 3 S. 1 DSGVO)	<ul style="list-style-type: none"> - Bürgerinnen und Bürger - Unternehmensmitarbeiter/-innen - Behördenmitarbeiter/-innen
4. ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (siehe z. B. Art. 30 Abs. 1 S. 2 lit. e DSGVO)	<ul style="list-style-type: none"> - im Fall von Online-Diensten, die das ePayment der Plattform nutzen, können je nach Dienst im Verwendungszweck personenbezogene Daten enthalten sein, die an den Payment Provider übermittelt werden, der in einem Drittland angesiedelt ein kann (derzeit mit Sitz in der Schweiz)

¹ Es handelt sich hierbei um gesetzliche Muss-Angaben sowohl bei Auftragsverarbeitung, die der Verordnung (EU) 2016/679 (DSGVO) unterliegt wie auch bei Auftragsverarbeitung, welche den bundes- oder landesrechtlichen Vorschriften zur Umsetzung der Richtlinie (EU) 2016/680 unterliegt. Diese Angaben sind in gleicher Form gesetzlicher Muss-Bestandteil des vom Verantwortlichen zu erstellenden Verzeichnisses aller Verarbeitungstätigkeiten (vgl. Art. 30 Abs.1 DSGVO bzw. die inhaltlich entsprechenden Bestimmungen in den LDSG'en zur Umsetzung der Richtlinie (EU) 2016/680

Die Datenverarbeitung erfolgt auftragsgemäß in einem der Dataport-Rechenzentren. Diese sind gemäß ISO 27001 zertifiziert (umfasst das ISMS Information Security Management System von Dataport, die Infrastruktur der beiden Rechenzentren sowie die Netz- und Dienstinfrastruktur für den technischen Verfahrensbetrieb von Verwaltungsverfahren). Die Zertifizierung und ihre Gültigkeit (BSI-IGZ-0405-2020 Rechenzentrumsbetrieb und BSI-IGZ-0365-2019 Verfahrensdienste mit Middlewarebetrieb) können Sie hier öffentlich einsehen:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Managementsystemen/ISO-27001-Basis-IT-Grundschutz/ErteilteZertifikate/iso27001zertifikate_node.html.

Das Land Schleswig-Holstein hat den grundschutzkonformen Betrieb der OSI-Plattform inklusive des Bürgerportals und Servicekontos gemäß BSI-Grundschutz beauftragt. Entsprechend hat sich Dataport dem Maßnahmenkatalog verpflichtet, der hier veröffentlicht ist: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompodium/it-grundschutz-kompodium_node.html

2. Ihr Antrag auf weitere Veröffentlichung von Informationen über die technischen und organisatorischen Maßnahmen u.a. zum Schutz der Verarbeitung personenbezogener Daten wird im Übrigen gemäß § 9 Abs. 1 Nr. 1 IZG SH abgelehnt.

Die Weitergabe der Vertragsunterlagen würde technische Details in der Maßnahmenumsetzung erkennbar machen. Die Vertragsunterlagen enthalten verfahrensspezifische Details, die für einen Angriff nutzbar wären, beispielsweise

- Angaben über Dienste-Verfügbarkeiten und
- Nennung von technischen Details bei der Beschreibung der Businessprozesse wie die Integration des Governikus oder maximale Durchsatzraten,

die z.B. interessant zur Planung von Distributed Denial of Service Angriffe (DDOS) wären. Aufgrund der Sensibilität der über die Plattform und der Plattformdienste verarbeiteten Daten sowie der grundsätzlichen Bedeutung der Plattform und der Dienste für die Funktionsfähigkeit der digitalen Verwaltungsleistungen, ist die Beschränkung der Auskunft gerechtfertigt. Durch die Information über die Gegenstände der vertraglichen Regelungen und Zertifizierungen der für die Umsetzung des OZG genutzten Infrastrukturen von Dataport, kann Ihr Informationsinteresse und der Schutz der entsprechenden Infrastrukturen hinreichend Rechnung getragen werden.

3. Von der Schwärzung der Vertragsunterlagen wurde wegen des Umfangs der Anlagen (90 Seiten) und des damit für Sie gebührenpflichtigen Aufwandes abgesehen, da sie in Ihrem Schreiben vom 01.09.2021 nicht zu erkennen gegeben haben, mögliche Kosten tragen zu wollen. Gründe, die für eine Befreiung gemäß §2 IZG-SH-KostenVO sprechen, haben Sie nicht dargelegt und sind von Amts wegen nicht erkennbar. Dem öffentlichen Interesse an der Herstellung von Transparenz über die Maßnahmen der Datensicherheit

und des Datenschutzes bei dem Betrieb der Plattform und der darauf laufenden Dienste wird durch die hiermit erteilte Auskunft hinreichend Rechnung getragen.

4. Bezüglich der von Ihnen in Ihrer initialen Anfrage gestellten Anspruch auf Auskunft zu den hinter dem Entwurf einer Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (IT-Sicherheitsverordnung Portalverbund) – PVV stehenden Konzepten verweise ich Sie gemäß § 4 Abs. 3 S. 2 IZG SH an das insoweit zuständige Bundesministerium des Inneren, für Bau und Heimat.

Gemäß § 6 Abs. 4 IZG SH weise ich Sie wegen der teilweisen Versagung des Zugangs auf die Möglichkeit der Beschwerde gemäß § 14 IZG SH bei der Landesbeauftragten für Datenschutz, Postfach 71 16, 24171 Kiel, mail@datenschutzzentrum.de hin.

Mit freundlichen Grüßen



Gegen die Entscheidung können Sie innerhalb eines Monats nach Bekanntgabe beim Ministerium für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung, - Referat V 30 Grundsatzangelegenheiten Digitalisierung und E-Government - Postfach 7151, 24171 Kiel, digitalisierung@melund.landsh.de Widerspruch einlegen.