

Von: [Transparenzgesetz](#)
An: [Mailbox \(HmbBfDI\)](#)
Betreff: WG: [SPAMVERDACHT]Sicherheit des Verwaltungsportals [#233299]
Datum: Freitag, 19. November 2021 13:12:51

Von: Christina Franke [#233299]

Gesendet: Freitag, 19. November 2021 13:12:49 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: Transparenzgesetz

Betreff: [SPAMVERDACHT]Sicherheit des Verwaltungsportals [#233299]

Hamburgischen Transparenzgesetz (HmbTG) / Beschwerde nach Artikel 77 DSGVO

Sehr geehrte Damen und Herren,

Ich muss anzweifeln, dass die Verantwortlichen der Verwaltungsportale ein dem Stand der Technik entsprechende Sicherheit gewährleisten und mich dementsprechend über die Verwaltungsportale beschweren. Ich verweise auf <https://fragdenstaat.de/anfrage/verschlüsselung-un-sicherheit-der-verwaltungsportale/> und <https://fragdenstaat.de/anfrage/verschlüsselung-im-bsi-grundschutz/> und lege Beschwerde wegen Verstoß gegen Artikel 32 DSGVO ein.

Abgesehen von der aller Wahrscheinlichkeit nach fehlenden Verschlüsselung sind mir weitere Mängel aufgefallen, die ich ebenfalls in <https://fragdenstaat.de/anfrage/verschlüsselung-un-sicherheit-der-verwaltungsportale/> aufgezählt habe. Im Fall Hamburg sind das

- * eine abweichende Domäne zwischen Portal und gesendeten Emails,
- * die Verpflichtung zum Postfach.

Darüberhinaus halte ich die Datenschutzerklärung für fragwürdig, denn sie gibt die Rechtsgrundlagen der Datenverarbeitung nicht korrekt wieder.

Da meines Wissens Auftragsverarbeiter beauftragt sind, bitte ich Sie auch zu prüfen ob entsprechend Artikel 28 DSGVO entsprechende Verträge geschlossen wurden. Die widerwilligen Antworten auf die Anfragen von Frau Maier - https://fragdenstaat.de/anfragen/?user=v.maier_3 - lassen mich vermuten, dass Verträge fehlen oder keine Artikel 32 DSGVO - Stand der Technik - erfüllenden TOMs enthalten.

Ausschlussgründe liegen meines Erachtens nicht vor. Sofern Teile der Information durch Ausschlussgründe geschützt sind, beantrage ich mir die nicht geschützten Teile zugänglich zu machen.

Ich bitte Sie zu prüfen, ob Sie mir die erbetene Auskunft auf elektronischem Wege kostenfrei erteilen können. Sollte die Aktenauskunft Ihres Erachtens in jedem Fall gebührenpflichtig sein, möchte ich Sie bitten, mir dies vorab mitzuteilen und dabei die Höhe der Kosten anzugeben.

Ich verweise auf § 13 Abs. 1 HmbTG und bitte Sie, mir die erbetenen Informationen unverzüglich und nur im Ausnahmefall spätestens nach Ablauf eines Monats nach Antragszugang zugänglich zu machen.

Sollten Sie für diesen Antrag nicht zuständig sein, bitte ich Sie, ihn an die zuständige Behörde weiterzuleiten und mich darüber zu unterrichten. Ich widerspreche ausdrücklich der Weitergabe meiner Daten an Dritte.

Ich möchte Sie um eine Antwort in elektronischer Form (E-Mail) bitten und bitte Sie um eine Empfangsbestätigung. Danke für Ihre Mühe!

Mit freundlichen Grüßen

Christina Franke

Anfragen: 233299

Antwort an: c.franke.6.zhufhu83u@fragdenstaat.de

Laden Sie große Dateien zu dieser Anfrage hier hoch:

<https://fragdenstaat.de/anfrage/233299/upload/06e680fa5f16aed3d7697fea7383b5a84e1dfdaa/>

Postanschrift

Christina Franke

Hirschstraße 152

76137 Karlsruhe

--

Rechtshinweis: Diese E-Mail wurde über den Webservice fragdenstaat.de versendet. Antworten werden ggf. im Auftrag der Antragstellenden auf dem Internet-Portal veröffentlicht.

Falls Sie Fragen dazu haben oder eine Idee, was für eine Anfrage bei Ihnen im Haus notwendig wäre, besuchen Sie:

<https://fragdenstaat.de/fuer-behoerden/>

Von: [Wirth, Sebastian Dr.](#)
An: [Wallbraun, Swantje](#)
Betreff: WG: [SPAMVERDACHT]Sicherheit des Verwaltungsportals [#233299]
Datum: Dienstag, 7. Dezember 2021 10:29:00

Az.: 3627_2021

Hallo Swantje,

wie gerade besprochen hier die Transparenzanfrage.
Sobald ich weiß, ob wir zum Verwaltungsportal Unterlagen haben, maile ich dir den Stand und ggf. den Inhalt.
Die den Aspekt der nicht ausreichenden TOMs und der Datenschutzerklärung des Verwaltungsportals der SK
werde ich über die angegebene Mailadresse beantworten.

Gruß

Sebastian

--

Dr. Sebastian Wirth

Referat T

Referatsleiter für den technischen Datenschutz, T

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift:

Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsstelle:

Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

Durchwahl

Büro: +49 (0)40 428 54-4053

E-Mail

sebastian.wirth@datenschutz.hamburg.de

Webauftritt

datenschutz-hamburg.de

-----Ursprüngliche Nachricht-----

Von: Transparenzgesetz

Gesendet: Freitag, 19. November 2021 13:13

An: Mailbox (HmbBfDI) <mailbox@datenschutz.hamburg.de>

Betreff: WG: [SPAMVERDACHT]Sicherheit des Verwaltungsportals [#233299]

Von: Christina Franke [#233299]

Gesendet: Freitag, 19. November 2021 13:12:49 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: Transparenzgesetz

Betreff: [SPAMVERDACHT]Sicherheit des Verwaltungsportals [#233299]

Hamburgischen Transparenzgesetz (HmbTG) / Beschwerde nach Artikel 77 DSGVO

Sehr geehrte Damen und Herren,

Ich muss anzweifeln, dass die Verantwortlichen der Verwaltungsportale ein dem Stand der Technik entsprechende Sicherheit gewährleisten und mich dementsprechend über die Verwaltungsportale beschweren.

Ich verweise auf <https://fragdenstaat.de/anfrage/verschlüsselung-un-sicherheit-der-verwaltungsportale/> und <https://fragdenstaat.de/anfrage/verschlüsselung-im-bsi-grundschutz/> und lege Beschwerde wegen Verstoß gegen Artikel 32 DSGVO ein.

Abgesehen von der aller Wahrscheinlichkeit nach fehlenden Verschlüsselung sind mir weitere Mängel aufgefallen, die ich ebenfalls in <https://fragdenstaat.de/anfrage/verschlüsselung-un-sicherheit-der-verwaltungsportale/> aufgezählt habe. Im Fall Hamburg sind das

- * eine abweichende Domäne zwischen Portal und gesendeten Emails,
- * die Verpflichtung zum Postfach.

Darüberhinaus halte ich die Datenschutzerklärung für fragwürdig, denn sie gibt die Rechtsgrundlagen der Datenverarbeitung nicht korrekt wieder.

Da meines Wissens Auftragsverarbeiter beauftragt sind, bitte ich Sie auch zu prüfen ob entsprechend Artikel 28 DSGVO entsprechende Verträge geschlossen wurden. Die widerwilligen Antworten auf die Anfragen von Frau Maier - https://fragdenstaat.de/anfragen/?user=v.maier_3 - lassen mich vermuten, dass Verträge fehlen oder keine Artikel 32 DSGVO - Stand der Technik - erfüllenden TOMs enthalten.

Ausschlussgründe liegen meines Erachtens nicht vor. Sofern Teile der Information durch Ausschlussgründe geschützt sind, beantrage ich mir die nicht geschützten Teile zugänglich zu machen.

Ich bitte Sie zu prüfen, ob Sie mir die erbetene Auskunft auf elektronischem Wege kostenfrei erteilen können. Sollte die Aktenauskunft Ihres Erachtens in jedem Fall gebührenpflichtig sein, möchte ich Sie bitten, mir dies vorab mitzuteilen und dabei die Höhe der Kosten anzugeben.

Ich verweise auf § 13 Abs. 1 HmbTG und bitte Sie, mir die erbetenen Informationen unverzüglich und nur im Ausnahmefall spätestens nach Ablauf eines Monats nach Antragszugang zugänglich zu machen.

Sollten Sie für diesen Antrag nicht zuständig sein, bitte ich Sie, ihn an die zuständige Behörde weiterzuleiten und mich darüber zu unterrichten. Ich widerspreche ausdrücklich der Weitergabe meiner Daten an Dritte.

Ich möchte Sie um eine Antwort in elektronischer Form (E-Mail) bitten und bitte Sie um eine Empfangsbestätigung. Danke für Ihre Mühe!

Mit freundlichen Grüßen
Christina Franke

Anfragenr: 233299
Antwort an: c.franke.6.zhufhf83u@fragdenstaat.de

Laden Sie große Dateien zu dieser Anfrage hier hoch:
<https://fragdenstaat.de/anfrage/233299/upload/06e680fa5f16aed3d7697fea7383b5a84e1dfdaa/>

Postanschrift
Christina Franke
Hirschstraße 152
76137 Karlsruhe

--

Rechtshinweis: Diese E-Mail wurde über den Webservice fragdenstaat.de versendet. Antworten werden ggf. im Auftrag der Antragstellenden auf dem Internet-Portal veröffentlicht.

Falls Sie Fragen dazu haben oder eine Idee, was für eine Anfrage bei Ihnen im Haus notwendig wäre, besuchen Sie:

<https://fragdenstaat.de/fuer-behoerden/>



Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

T / Dr. Sebastian Wirth
Az.: 3627/2021

12.01.2022

Domänen bei der Registrierung in OSI

Die Registrierung eines Nutzerkontos in OSI erfolgt unter <https://servicekonto.serviceportal.hamburg.de/servicekonto/>

noreply_serviceportal-hamburg@dataport.de zur Aktivierung des Nutzerkontos in OSI per-Link nach der ersten Registrierung im Nutzerkonto.

Der Sachverhalt, den die Petentin kritisiert, dass sich die Domäne des Nutzerkontos und des Absenders der Mail mit dem verschickten Aktivierungs-Links sich unterscheiden stimmt.

In der Datenschutzerklärung und in den Hilfetexten von A-Z des Serviceportals wird jedoch die Mailadresse meinserviceportal@dataport.de explizit als Kontaktadresse für Fragen zur Registrierung zum Nutzerkonto genannt. Diese Mailadresse für Fragen zur Registrierung ist derselben Domäne wie die Mail, mit der das Nutzerkonto aktiviert werden muss. Die Nutzer:innen können somit leicht die Herkunft der Mail beim Registrierungsprozess nachvollziehen.

Dr. Sebastian Wirth

Informationen zum Datenschutz nach der EU Datenschutz-Grundverordnung (DS-GVO)

Datenschutzerklärung

Nahezu alle Bürgerinnen und Bürger sowie Unternehmen treten mit der Verwaltung früher oder später in Kontakt, weil sie z.B. einen Personalausweis beantragen müssen oder Kindergeld beanspruchen können. Hierbei müssen personenbezogene Daten verarbeitet werden.

In einem Verwaltungsverfahren sind Daten personenbezogen, wenn sie einer natürlichen Person zugeordnet werden können. Keine personenbezogenen Daten sind anonymisierte Daten.

Wenn Verwaltungsbehörden personenbezogene Daten verarbeiten, bedeutet das, dass sie diese Daten z. B. erheben, speichern, verwenden, übermitteln, zum Abruf bereitstellen oder löschen.

Die Daten werden nur für den Zweck verwendet, für den sie erhoben wurden. Eine Weitergabe erfolgt an die von Ihnen gewählten und tatsächlich genutzten Online-Dienste im Hamburg Serviceportal. Im Rahmen des Onlinezugangsgesetzes (OZG) ist es auch möglich, dass Sie Online-Verwaltungsdienste des Bundes oder anderer Bundesländer über das Hamburg Service-Portal beantragen. Werden Dienste von Behörden erbracht, die nicht zur Freien und Hansestadt Hamburg gehören, übermitteln wir Ihre Daten an die für die beantragte Verwaltungsleistung zuständige Stelle. Wann das der Fall ist, schildern wir unter der Rubrik: „Unter welchen Voraussetzungen dürfen wir Ihre Daten an Dritte weitergeben“.

Im Folgenden informieren wir Sie darüber, welche personenbezogenen Daten wir erheben, bei wem wir sie erheben und was wir mit diesen Daten machen. Außerdem informieren wir Sie über Ihre Rechte in Datenschutzfragen und an wen Sie sich diesbezüglich wenden können.

Inhaltsverzeichnis

[Wer sind wir?](#)

[Wer sind Ihre Ansprechpartner?](#)

[Warum und zu welchem Zweck verarbeiten wir Ihre personenbezogenen Daten?](#)

[Welche personenbezogenen Daten verarbeiten wir?](#)

[Wie verarbeiten wir diese Daten?](#)

[Unter welchen Voraussetzungen dürfen wir Ihre Daten an Dritte weitergeben?](#)

[Wie lange speichern wir Ihre Daten?](#)

[Welche Rechte \(Auskunftsrecht, Widerspruchsrecht usw.\) haben Sie?](#)

Wer sind wir?

Das **Hamburg Serviceportal** der Freien und Hansestadt Hamburg bietet einen sicheren Zugang zu den Online-Diensten der Stadt. Es bietet Ihnen Funktionen, mit denen Sie Online-Dienstleistungen suchen und finden, sich für die Nutzung von Online-Diensten registrieren und anmelden sowie in Bezug auf genutzte Online-Dienste sicher mit der Verwaltung kommunizieren können.

Damit wir die gewünschten Leistungen für Sie erbringen können, ist es bei vielen Online-Diensten erforderlich, dass Sie Ihre Daten zur Verfügung stellen. Wir verarbeiten diese Daten nur im Rahmen Ihres Auftrags und verwenden sie nur unter Beachtung der gesetzlichen Bestimmungen (Onlinezugangsgesetz (OZG), Hamburgisches Datenschutzgesetz, EU Datenschutzgrundverordnung (DSGVO), Telekommunikationsgesetz, Telemediengesetz sowie einschlägige Fachgesetze wie beispielsweise das Meldegesetz).

Online-Dienste im Hamburg Serviceportal

Die untenstehenden Informationen beziehen sich auf das Hamburg Serviceportal, insbesondere auf die Benutzerkonten (Servicekonten) und Servicekonto-Postfächer. Informationen zu den einzelnen Online-Diensten finden Sie bei den [Informationen zum Datenschutz bei der Verwendung von Online-Diensten](#).

Wer sind Ihre Ansprechpartner?

Fragen in datenschutzrechtlichen Angelegenheiten können Sie an den für die Servicekonten und das Portal zuständigen Datenschutzbeauftragten der Senatskanzlei richten:

Senat der Freien und Hansestadt Hamburg
Datenschutzbeauftragter der Senatskanzlei
Hermannstraße 15, 20095 Hamburg
Tel.: +49 40 42831 – 2500
E-Mail: behoerdlicherdatenschutz@sk.hamburg.de

Falls Sie Fragen zur Registrierung oder Anmeldung haben oder uns Ihre Anregungen oder Hinweise zum Serviceportal mitteilen möchten, nehmen Sie bitte unter der E-Mail-Adresse meinserviceportal@dataport.de Kontakt zu uns auf.

Freie und Hansestadt Hamburg
Senatskanzlei
Amt für IT und Digitalisierung
Fachliche Leitstelle für den HamburgService / das Hamburg Serviceportal
Rathausmarkt 1, 20095 Hamburg
Telefon: +49 40 42823 – 2500
E-Mail: meinserviceportal@dataport.de

Warum und zu welchem Zweck verarbeiten wir Ihre personenbezogenen Daten?

Wir verarbeiten Ihre personenbezogenen Daten, damit Sie die über das Service-Portal angebotenen Verwaltungsleistungen online in Anspruch nehmen können (Verarbeitungszweck).

Im Hamburg Serviceportal werden Ihre Daten zunächst zur Einrichtung eines Benutzerkontos (Servicekonto) verarbeitet. Ein Servicekonto ist zur Nutzung der zur Verfügung gestellten Online-Dienste erforderlich. Wenn Sie dann Online-Dienste über Ihr Nutzerkonto beanspruchen, übermitteln

wir Ihre Daten an die zuständige Fachbehörde. Ihre einmalige Einwilligung ist grundlegend für die Verarbeitung Ihrer Daten für alle Online-Dienste der Stadt, die Sie aus Ihrem Nutzerkonto über das Service-Portal abwickeln möchten.

Im Rahmen des Online-Zugangsgesetzes liegt die Verantwortlichkeit für die Verarbeitung Ihrer Daten in bestimmten Fällen auch zusätzlich in anderen Bundesländern, an die Ihre Daten dann für die Nutzung eines solchen Online-Dienstes übermittelt werden. Vor einer Übermittlung fragen wir Ihre Einwilligung in jedem Einzelfall ab.

Zu jedem Servicekonto gehört ein Postfach, damit Sie im Zusammenhang mit der Nutzung von Online-Diensten sicher mit der Verwaltung kommunizieren können. Die Verarbeitung von Daten des Servicekonto-Postfachs erfolgt auf Basis Ihrer Einwilligung und aufgrund der Erfüllung rechtlicher Verpflichtungen sowie der einschlägigen Rechtsvorschriften der von Ihnen genutzten Online-Dienste. Auf das Postfach und die gespeicherten Nachrichten können nur Sie als Inhaber des Servicekontos nach einer Anmeldung am Servicekonto zugreifen. Welche personenbezogenen Daten in einer Postfachnachricht enthalten sind, hängt von der jeweiligen Nachricht und dem Online-Dienst ab, in dessen Zusammenhang die Nachricht verschickt wird.

Zur Gewährleistung der Funktionalität des Online-Dienstes ist es erforderlich, dass Ihre Daten an die jeweils zuständigen Behörden übermittelt werden und Sie dieser Übermittlung zugestimmt haben (Einwilligung). Der Zweck der Übermittlung Ihrer Daten besteht darin, dass Sie die von dem Onlinedienst angebotene Verwaltungsleistung in Anspruch nehmen können.

Sie sind nicht verpflichtet, diese Einwilligung zu erteilen. Sollten Sie Ihre Einwilligung nicht erteilen, erfolgt keine Übermittlung Ihrer Daten. Damit kann allerdings auch die von Ihnen begehrte Verwaltungsleistung über Ihr Nutzerkonto nicht in Anspruch genommen werden. Wenden Sie sich in diesem Fall direkt an die zuständige Behörde, Sie können die Verwaltungsleistung auch dort in nicht-elektronischer Weise in Anspruch nehmen.

Sie können Ihre Einwilligung jederzeit widerrufen. Dadurch wird allerdings die damit ausgelöste Übermittlung Ihrer Daten nicht rückgängig gemacht. Eine Löschung bzw. Sperrung Ihrer übermittelten Daten müssen Sie direkt bei der oben genannten verantwortlichen Stelle geltend machen.

Beispiele zur Verarbeitung:

Beispiel 1: Sie möchten einen Online-Dienst nutzen, der ein Servicekonto erfordert. Sie registrieren sich dazu im Serviceportal. Mit dem Abschluss der Registrierung besitzen Sie ein Servicekonto, in dem Daten zu Ihrer Person gespeichert sind (s. unten). Zu diesem Servicekonto gehört ein Postfach. Bei der Nutzung einiger Online-Dienste erhalten Sie z.B. eine Auskunft in Form einer Postfach-Nachricht in Ihr Postfach. Sie werden z.B. per E-Mail über den Eingang der Nachricht in ihr Postfach informiert. Um die Nachricht zu lesen, müssen Sie sich an Ihrem Servicekonto anmelden und in das Postfach navigieren.

Beispiel 2: Sie möchten einen Online-Dienst eines anderen Bundeslandes oder des Bundes nutzen. Sie können den Dienst online aufrufen und sich dann mit Ihrem Hamburger Servicekonto anmelden. Sobald Sie in die Übermittlung Ihrer Daten eingewilligt haben, werden die personenbezogenen Daten aus Ihrem Nutzerkonto an die verantwortliche Stelle des anderen Bundeslandes oder des Bundes übermittelt, die für den Betrieb des von Ihnen aufgerufenen Dienstes datenschutzrechtlich verantwortlich ist.

Welche personenbezogenen Daten verarbeiten wir?

Wir verarbeiten insbesondere folgende personenbezogene Daten:

Einfaches Servicekonto für Bürgerinnen und Bürger („Servicekonto“)

Für die Nutzung von Online-Diensten mit dem Kontotyp einfaches „Servicekonto“ speichern wir nach Ihrer Zustimmung folgende personenbezogene Daten:

1. Vorname
2. Nachname
3. E-Mail-Adresse
4. Passwort
5. Wahl der Darstellungssprache (derzeit immer „Deutsch“)
6. Servicekontotyp (freigeschaltete Sicherheitsstufe)
7. Datum der Einwilligung zur Datenverarbeitung

Servicekonto mit Identifikationsnachweis für Bürgerinnen und Bürger („Servicekonto Plus“)

Für die Nutzung von Online-Diensten mit dem Kontotyp „Servicekonto Plus“ speichern wir nach Ihrer Zustimmung folgende personenbezogene Daten:

1. Vorname
2. Nachname
3. Adresse (Straße, Hausnummer, PLZ, Ort, Land)
4. Geburtsdatum
5. Geburtsname
6. Geburtsort
7. E-Mail-Adresse
8. Passwort
9. Wahl der Darstellungssprache (derzeit immer „Deutsch“)
10. Servicekontotyp (freigeschaltete Sicherheitsstufe)
11. Datum der Einwilligung zur Datenverarbeitung

Daten, die Sie als Bürgerin oder Bürger zusätzlich angeben können

Sie haben die Möglichkeit, weitere Daten in Ihrem Servicekonto zu hinterlegen. Diese Daten werden in manchen Online-Diensten dazu verwendet, Felder in Formularen vorauszufüllen, um Ihnen die Eingabe zu ersparen.

Wenn Sie ein einfaches Servicekonto besitzen („Servicekonto“), können Sie optional auch die Daten für das „Servicekonto Plus“ ausfüllen (s. oben).

Sowohl für das „Servicekonto“ als auch das „Servicekonto Plus“ können Sie folgende Daten zusätzlich angeben:

1. Anrede
2. Akademischer Titel
3. Adresszusatz
4. Telefonnummer
5. Mobiltelefonnummer

Hinterlegung Ihrer Zahlungsdaten beim Payment Provider zur Wiederverwendung bei Zahlungsvorgängen mit ePayment

Bei Online-Dienstleistungen, die Sie online per ePayment bezahlen können, haben Sie die Möglichkeit, die einmal angegebenen Zahlungsdaten (z.B. Ihre Kontodaten) beim Payment Provider speichern zu lassen. In diesem Fall wird in Ihrem Servicekonto eine Referenznummer des Payment

Providers gespeichert. Die beim Payment Provider gespeicherten Daten können Sie bei späteren Zahlungsvorgängen wiederverwenden, sodass Sie die Daten nicht erneut eingeben müssen.

Ab 2021 erfolgt ein Umstieg auf die von der Entwicklergemeinschaft Bund-Länder entwickelte Zahlungskomponente ePayBL. Bei dieser Zahlkomponente werden die Zahlungsdaten nicht beim Payment Provider hinterlegt.

Registrierung eines Servicekontos für Bürgerinnen und Bürger mithilfe der eID-Funktion des Personalausweises

Wenn Sie sich mit der eID-Funktion des Personalausweis registrieren, werden die Daten Nr. 1-6 vom Personalausweis ausgelesen und gespeichert, sofern Sie dem zugestimmt haben.

Zusätzlich wird das "Pseudonym" bzw. „Kartenkennung" Ihres Ausweises gespeichert, wenn Sie die Funktion "Anmelden mit Online-AusweisFunction" aktiviert haben.

Servicekonto für Unternehmen und andere Organisationen („Servicekonto Business“)

Bei Servicekonten für Unternehmen, Behörden und andere Organisationen sind unterschiedliche Daten zu unterscheiden: 1. Daten zum Unternehmen, 2. Daten zu Administratoren für das „Servicekonto Business“ und 3. Daten zu Mitarbeiterinnen und Mitarbeitern, die Online-Dienste nutzen.

Zum Unternehmen / zur Organisation

Folgende Daten werden zu Organisationen gespeichert:

1. Name der Organisation
2. Organisationsadresse (Straße, Hausnummer, PLZ, Ort, Land)
3. Freigeschaltete Online-Dienste
4. Nutzung von Online-Diensten durch die Administratoren

Zum Servicekonto-Administrator für das „Servicekonto Business“

Administratoren für ein „Servicekonto Business“ sind Nutzer im Unternehmen, die erweiterte Berechtigungen auf ein „Servicekonto Business“ besitzen und neben ihren eigenen Daten auch die Daten zum Unternehmen bzw. der Organisation ändern können. Sie können außerdem die Mitarbeiterinnen und Mitarbeiter des Unternehmens verwalten (einrichten, löschen, ändern und technisch berechtigen), die für das Unternehmen Online-Dienste nutzen. Zu Administratoren werden folgende Daten gespeichert:

1. Vorname
2. Nachname
3. E-Mail-Adresse
4. Passwort
5. Telefonnummer
6. Wahl der Darstellungssprache (derzeit immer „Deutsch“)
7. Servicekontotyp
8. Datum der Einwilligung zur Datenverarbeitung
9. Berechtigungsrollen in Online-Diensten

Zu Unternehmens- bzw. Organisationsmitarbeiterinnen und -mitarbeitern eines „Servicekonto Business“

Mitarbeiterinnen und Mitarbeiter des Unternehmens oder der Organisation werden vom Servicekonto-Administrator (s. oben) eingerichtet und verwaltet. Sie werden durch den Servicekonto-Administrator zur Nutzung von Online-Diensten im Namen des Unternehmens oder der Organisation technisch berechtigt. Zu Unternehmens- bzw. Organisationsmitarbeitern werden folgende Daten gespeichert:

1. Vorname
2. Nachname
3. E-Mail-Adresse
4. Passwort
5. Wahl der Darstellungssprache (derzeit immer „Deutsch“)
6. Servicekontotyp

Daten, die Sie für „Servicekonto Business“-Nutzer zusätzlich angeben können

Sie haben die Möglichkeit, weitere Daten in Ihrem „Servicekonto Business“ zu hinterlegen. Diese Daten werden in manchen Online-Diensten dazu verwendet, Felder in Formularen vorauszufüllen, um Ihnen die Eingabe zu ersparen:

1. Anrede
2. Akademischer Titel (zu Administratoren und Mitarbeiter/innen)
3. Organisationseinheit (zu Administratoren und Mitarbeiter/innen)
4. Faxnummer (bei Organisations-Administratoren)
5. Telefonnummer (bei Mitarbeiter/innen)
6. Mobiltelefonnummer (bei Administratoren und bei Mitarbeiter/innen)
7. Handelsregisternummer (zur Organisation)
8. E-Mail-Adresse der Organisation
9. Postfach-Nummer der Organisation
10. Postfach-PLZ der Organisation

Hinterlegung Ihrer Zahlungsdaten beim Payment Provider zur Wiederverwendung bei Zahlungsvorgängen mit ePayment

Sie haben die Möglichkeit, die einmal angegebenen Zahlungsdaten (z.B. Ihre Kontodaten) beim Payment Provider speichern zu lassen. In diesem Fall wird in Ihrem „Servicekonto Business“ eine Referenznummer des Payment Providers gespeichert. Die beim Payment Provider gespeicherten Daten können Sie bei späteren Zahlungsvorgängen wiederverwenden, sodass Sie die Daten nicht erneut eingeben müssen.

Ab 2021 erfolgt ein Umstieg auf die von der Entwicklergemeinschaft Bund-Länder entwickelte Zahlungskomponente ePayBL. Bei dieser Zahlkomponente werden die Zahlungsdaten nicht beim Payment Provider hinterlegt.

Wichtiger Hinweis zum Passwort

Halten Sie Ihr Passwort geheim, damit keine unberechtigten Personen Zugang zu Ihren Daten erlangen. Geben Sie Ihr Passwort nicht auf Nachfrage bekannt. Auch die technischen Betreuer des Hamburg Serviceportals sind nicht berechtigt, Ihr Passwort zu erfahren.

Servicekonto-Postfach

Wenn Sie ein Servicekonto nutzen, wird für Sie auch ein Servicekonto-Postfach angelegt. Für die Nutzung werden folgende Daten aus dem Servicekonto im Postfach-System gespeichert:

- Anrede
- Vorname

- Nachname
- E-Mail-Adresse
- Telefonnummer

Daneben werden innerhalb des Servicekonto-Postfachs die Nachrichtenkonversation zwischen Ihnen und den Behörden gespeichert. In den Nachrichten können personenbezogene Daten enthalten sein, dies ist abhängig davon, welche Verwaltungsleistung Sie nutzen.

Suchen & Finden des Online-Gateways Portalverbund

Wenn Sie im Suchfeld eine andere Stadt als Hamburg eingeben, wird die Suche durch das Online-Gateway Portalverbund ausgeführt. Mit dem Online-Gateway können Sie deutschlandweit nach Verwaltungsleistungen suchen. Die von Ihnen als Bürgerin oder Bürger während der Suche verarbeiteten Daten werden nicht gespeichert und nicht weiterverarbeitet. Der Zugriff auf die Suchfunktion erfolgt pseudonym. Es wird keine Suchhistorie und auch keine Historie der Vervollständigung der Begriffe erstellt. Es erfolgt keine Verknüpfung mit Ihren bestehenden Benutzerkonten aus den Verwaltungsportalen (Servicekonten).

Ihre IP-Adresse und der verwendete Internet-Browser werden in technischen Protokollen (Logfiles) erfasst. Die Notwendigkeit der Speicherung dieser Daten ergibt sich aus den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik. Dabei erfolgt im Regelfall eine Speicherung für drei Tage. Bei Auffälligkeiten der Aufrufe werden die Daten zur Analyse für maximal 1 Jahr sicher aufbewahrt.

Wie verarbeiten wir diese Daten?

Ihre personenbezogenen Daten werden gespeichert. Sofern Sie an Ihrem Servicekonto angemeldet sind, werden die Daten aus Ihrem Servicekonto in bestimmten Online-Diensten dazu genutzt, Formularfelder vorauszufüllen, so dass Sie diese Daten nicht erneut eingeben müssen. Erst wenn Sie eine explizite Aktion wie z.B. das Senden eines von Ihnen ausgefüllten Online-Formulars (i.d.R durch einen Klick auf eine entsprechend bezeichnete Schaltfläche) ausführen, werden diese Daten in das dem Online-Dienst zugeordnete Verwaltungsverfahren übernommen.

Wir setzen technische und organisatorische Sicherheitsmaßnahmen ein, um Ihre personenbezogenen Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust oder Veränderung sowie gegen unbefugte Offenlegung oder unbefugten Zugang zu schützen. Unsere Sicherheitsstandards entsprechen stets den aktuellsten technologischen Entwicklungen.

Unter welchen Voraussetzungen dürfen wir Ihre Daten an Dritte weitergeben?

Alle personenbezogenen Daten, die uns in einem Verwaltungsverfahren bekannt geworden sind, dürfen wir nur dann an andere Personen oder Stellen weitergeben, wenn Sie der Weitergabe zugestimmt haben oder die Weitergabe gesetzlich zugelassen ist.

Werden Dienste von Behörden erbracht, die nicht zur Freien und Hansestadt Hamburg gehören, so wird Ihnen dies deutlich angezeigt. Bund und Länder haben sich nach dem Onlinezugangsgesetz (OZG) zusammengeschlossen, um den Bürgern elektronisch Verwaltungsleistungen anbieten zu können. Mit Ihrem Hamburger Benutzerkonto können Sie die Leistungen andere Portale des Bundes und der Länder nutzen. In einem solchen Fall werden Ihre Daten an die bearbeitende Stelle weitergegeben. Sie werden im Einzelfall vor einer solchen Weitergabe informiert und müssen ihr auch zustimmen.

Damit Sie Online-Dienste eines anderen Bundeslandes oder des Bundes mit Ihrem Konto nutzen können, haben die Verantwortlichen für die Nutzerkonten der Bundesländer und des Bundes gemeinsame Vorgehensweisen, Datenflüsse und die Festlegung von technischen Anforderungen in einer Verwaltungsvereinbarung festgeschrieben. Diese regelt auch die Verantwortlichkeiten bei der Verarbeitung Ihrer personenbezogenen Daten, wenn Sie Online-Dienste anderer Bundesländer mit Ihrem Nutzerkonto nutzen. Es ist somit nicht erforderlich, dass Sie in dem anderen Bundesland bzw. beim Bund ein zusätzliches Nutzerkonto anlegen. Näheres erfahren Sie [hier](#).

Eine Datenübermittlung an Dritte findet auch beim ePayment statt. Das Rechenzentrum des derzeitigen Payment-Providers „SIX Payment Services (Germany) GmbH“ befindet sich in der Schweiz. Das Datenschutzniveau in der Schweiz wurde von der EU als gleichwertig anerkannt. Je nach Online-Dienstleistung können im Verwendungszweck des Zahlungsvorgangs personenbezogene Daten übertragen werden (z.B. ein Aktenzeichen oder andere fachliche Referenznummer).

Ab 2021 erfolgt ein Umstieg auf die von der Entwicklergemeinschaft Bund-Länder entwickelte Zahlungskomponente ePayBL. Das Hosting von ePayBL erfolgt durch den SID (Staatsbetrieb Sächsische Informatik Dienste), die ihre Rechenzentren PCI-DSS-konform betreiben und entsprechend der Sensibilität der vorliegenden Daten unter Berücksichtigung hoher Datenschutzauflagen handeln. Der Payment Provider ist dann PAYONE Girosolution. Der Payment Provider unterliegt der Regulierung des Bankengeschäfts und den damit verbundenen Sicherheitsstandards.

Wie lange speichern wir Ihre Daten?

Servicekonto

Wir speichern Ihre Daten in Ihrem Servicekonto, solange Sie es nutzen. Wenn Sie Ihr Servicekonto eine festgelegte Zeit lang nicht nutzen, wird es gelöscht: Im Fall des „Servicekonto Plus“ und „Servicekonto Business“ beträgt der Zeitraum fünf Jahre, im Fall einfacherer Servicekonten zwei Jahre. Vor der endgültigen Löschung weist das System Sie per E-Mail darauf hin, dass Ihr Servicekonto inklusive Postfach und aller enthaltenen Postfach-Nachrichten gelöscht werden wird, sofern Sie sich nicht erneut am Servicekonto anmelden.

Servicekonto-Postfach

Die Postfachnachrichten werden gespeichert, bis sie gelöscht werden. Die Löschung erfolgt ausschließlich durch Sie. Eine automatische Löschung der Postfachnachrichten erfolgt nicht, allerdings werden alle Postfachnachrichten gelöscht, wenn das zugrundeliegende Servicekonto gelöscht wird.

Welche Rechte (Auskunftsrecht, Widerspruchsrecht usw.) haben Sie?

Sie haben nach der Datenschutz-Grundverordnung verschiedene Rechte. Einzelheiten ergeben sich insbesondere aus Artikel 15 bis 18 und 21 der Datenschutz-Grundverordnung.

Recht auf Auskunft

Sie können Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten verlangen. In Ihrem Auskunftsantrag sollten Sie Ihr Anliegen präzisieren, um uns das Zusammenstellen der erforderlichen Daten zu erleichtern. Daher sollten in dem Antrag möglichst Angaben zum konkreten Verwaltungsverfahren und zum Verfahrensabschnitt gemacht werden.

Recht auf Berichtigung

Sollten die Sie betreffenden Angaben nicht (mehr) zutreffend sein, können Sie eine Berichtigung verlangen. Sollten Ihre Daten unvollständig sein, können Sie eine Vervollständigung verlangen.

Recht auf Löschung

Sie können die Löschung Ihrer personenbezogenen Daten verlangen. Ihr Anspruch auf Löschung hängt u. a. davon ab, ob die Sie betreffenden Daten von uns zur Erfüllung unserer gesetzlichen Aufgaben noch benötigt werden.

Die Löschung Ihrer Daten erfolgt in diesem Fall unverzüglich.

Recht auf Einschränkung der Verarbeitung

Sie haben das Recht, eine Einschränkung der Verarbeitung der Sie betreffenden Daten zu verlangen. Die Einschränkung steht einer Verarbeitung nicht entgegen, soweit an der Verarbeitung ein wichtiges öffentliches Interesse besteht.

Recht auf Widerspruch

Sofern Ihre Daten nicht auf der Grundlage Ihrer Einwilligung, sondern aus Gründen eines überwiegenden öffentlichen Interesses oder einer Rechtsvorschrift verarbeitet werden, haben Sie das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit der Verarbeitung der Sie betreffenden Daten zu widersprechen.

Recht auf Beschwerde

Wenn Sie der Auffassung sind, dass wir Ihrem Anliegen nicht oder nicht in vollem Umfang nachgekommen sind, können Sie bei der zuständigen Datenschutzaufsichtsbehörde Beschwerde einlegen:

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str 22, 7. OG, 20459 Hamburg
Tel.: (040) 4 28 54 - 40 40
E-Fax: (040) 4 279 – 11811
E-Mail: mailbox@datenschutz.hamburg.de

Allgemeine Hinweise zu diesen Rechten

In einigen Fällen können oder dürfen wir Ihrem Anliegen nicht entsprechen. Sofern dies gesetzlich zulässig ist, teilen wir Ihnen in diesem Fall immer den Grund für die Verweigerung mit.

Wir werden Ihnen aber grundsätzlich innerhalb eines Monats nach Eingang Ihres Anliegens antworten. Sollten wir länger als einen Monat für eine abschließende Klärung brauchen, erhalten Sie eine Zwischennachricht.

Informationen zu Cookies und Messverfahren zur Nutzung des Hamburg Serviceportals

Cookies

Cookies sind Datenelemente, die eine Website an Ihren Browser schickt, um sie auf Ihrem System zu speichern. Wir benutzen technisch notwendige "Sitzungs-Cookies", um Informationen aus der Website an Ihre Bedürfnisse anpassen zu können. Sobald Sie sich abmelden, werden die Cookies gelöscht.

Die meisten Browser können Sie so einstellen, dass Sie benachrichtigt werden, wenn Sie Cookies erhalten. Sie können dann selbst entscheiden, ob Sie das akzeptieren wollen oder nicht. Um den HamburgService nutzen zu können, müssen Sie diese Sitzungs-Cookies zulassen.

Stand 5. Mai 2021

Servicekonto-Registrierung

[Ihre Daten](#)[Zusammenfassung](#)

Zusammenfassung

Bitte überprüfen Sie Ihre Eingaben.

Ihre Daten

test Test

[Bearbeiten](#)

test.test@hamburg.de

Beachten Sie die [Datenschutzerklärung](#) zum Hamburg Serviceportal.

Ich habe die [Datenschutzerklärung](#) zur Kenntnis genommen und willige in die Verarbeitung meiner personenbezogenen Daten im Rahmen des Hamburg Serviceportals ein.

Von: [Wirth, Sebastian Dr.](#)
An: [Wagner, Felix](#)
Betreff: Eingabe Sicherheit der Veraltungsportale
Datum: Montag, 17. Januar 2022 16:09:11
Anlagen: [20220117_Schellungnahme_HmbBfDI_Entwurf_T.DOCX](#)
[Informationen zum Datenschutz nach der EU Datenschutz-Grundverordnung \(D...pdf](#)
[LDA_Bbq_AIG_233296_Beschwerde.pdf](#)
[20211116_Eingabe_beim_BfDI_Antwort_geschwärzt.pdf](#)
[WG_SPAMVERDACHTSicherheit_des_Verwaltungsportals_#233299.msg](#)

Az.: 3627/2021

Hallo Felix,

wir haben eine Eingabe zum hamburgischen Serviceportal bekommen, in der auch bezogen auf die Datenschutzerklärung kritisiert wird, dass dort die Rechtsgrundlage nicht konkret genug benannt wird. Im Entwurf der Stellungnahme habe ich die Passagen dazu eingefügt. Hältst du das für ausreichend oder ist es erforderlich, in der Datenschutzerklärung explizit § 8 OZG in Verbindung mit Art. 6 Abs. 1 Lit. e) DSGVO zu benennen?

Gruß
Sebastian

--

Dr. Sebastian Wirth

Referat T
Referatsleiter für den technischen Datenschutz, T

Freie und Hansestadt Hamburg
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg
Geschäftsstelle: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

Durchwahl Büro: +49 (0)40 428 54-4053
E-Mail sebastian.wirth@datenschutz.hamburg.de
Webauftritt datenschutz-hamburg.de

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.



Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg

Frau

Ludwig-Erhard-Str. 22, 7. OG
20459 Hamburg
Telefon: 040 - 428 54 - 40 53 Zentrale - 40 40
Telefax: 040 - 428 54 - 40 00
Ansprechpartner: Herr Dr. Sebastian Wirth
Referat T (Technik)
E-Mail*: Sebastian.Wirth@datenschutz.hamburg.de

Az.: T / 3627_2021

Hamburg, den ?? .2022.2020

nur per Mail

Sicherheit des Hamburgischen Verwaltungsportals

Guten Tag Frau XXXX,

vielen Dank für Ihre Nachricht vom 19.11.2021 in der Sie Bedenken äußern, dass bei Nutzerkonto im hamburgischen Serviceportal die erforderlichen Maßnahmen nach Art 23 DSGVO nicht erfüllt werden. Hierzu möchte ich zu den Aspekten Stellung nehmen, die Sie in Bezug auf das Servicekonto Hamburg in Ihrer Eingabe aufgeführt haben.

Abweichung der Domänen zwischen Portal und Mail-Domäne

Die Registrierung eines Nutzerkontos in OSI erfolgt unter <https://servicekonto.serviceportal.hamburg.de/servicekonto/>. Nach der ersten Registrierung erhalten die Nutzer:innen im Nutzerkonto zur Aktivierung des Nutzerkontos in OSI einer Link per Mail mit der Absender-Adresse noreply_serviceportal-hamburg@dataport.de .

Die Domäne des Nutzerkontos und des Absenders der Mail mit dem verschickten Aktivierungs-Links unterscheiden sich. In der Datenschutzerklärung und in den Hilfetexten von A-Z des Serviceportals wird jedoch die Mailadresse meinserviceportal@dataport.de explizit als Kontaktadresse für Fragen zur Registrierung zum Nutzerkonto genannt. Diese Mailadresse für Fragen zur Registrierung kommt aus derselben Domäne wie die Mail, mit der das Nutzerkonto aktiviert werden muss. Die Nutzer:innen können somit leicht die Herkunft der Mail beim Registrierungsprozess nachvollziehen.

Verpflichtung zum Postfach

Website:
www.datenschutz-hamburg.de

E-Mail Sammelpostfach*:
mailbox@datenschutz.hamburg.de

Öffentliche Verkehrsmittel:
S-Bahnen S1, S2, S3 (Station Stadthausbrücke),
U-Bahn U3 (Station St. Pauli), Busse 6 und 37

*Vertrauliche Informationen sollten auf elektronischem Weg nur verschlüsselt an uns übermittelt werden.
Unser öffentlicher PGP-Schlüssel ist im Internet verfügbar (Fingerprint: 0932 579B 33C1 8C21 6C9D E77D 08DD BAE4 3377 5707)

Die Rechtsgrundlage der Verarbeitung der Daten in den Nutzerkonten und den Postfächern ist das Online-Zugangsgesetz, insbesondere in den §2 Abs. 7, §8 Abs. 4 und §9 Abs. 1. OZG. Diese gesetzlichen Grundlagen der Datenverarbeitung inkorporieren die Einwilligungen bzw. Zustimmungen als bloßes Tatbestandsmerkmale. Die Rechtsgrundlage der Verarbeitung ist somit nicht die Einwilligung gemäß Art. 6 Abs. 1a DSGVO.

Das OZG wurde bezüglich der Postfächer im Dezember 2020 geändert. In der Bundestagsdrucksache Drucksache 19/23774 vom 28.10.2020 ist in der Begründung zu dieser Änderung unter Ziffer Zu Nummer 1 Buchstabe d ausgeführt:

"Eine vollständige Kommunikation zwischen Nutzern und der Verwaltung umfasst nicht nur die Beantragung einer Verwaltungsleistung, sondern auch den sog. Rückkanal, insbesondere also die digitale Übermittlung der Entscheidung der Behörde an den Nutzer (bidirektionale Kommunikation). Hierzu stellen Bund und Länder im Rahmen des Aufbaus der Nutzerkonten sog. Postfächer bereit. Postfächer sind ein wesentlicher Basisdienst, um Mitteilungen, Bescheide und Benachrichtigungen zum Bearbeitungsstatus medienbruchfrei und nutzerfreundlich elektronisch bereitzustellen, die anschließend vom Nutzer abgerufen werden können. Die Kenntnisnahme bzw. das Herunterladen dieser Informationen durch den Nutzer setzt eine dem Vertrauensniveau der Verwaltungsleistung angemessene Authentisierung voraus. Das Postfach wurde bisher lediglich in der amtlichen Begründung zum OZG erwähnt und wird daher mit dieser Änderung in die Begriffsbestimmungen des OZG aufgenommen. Die Gestaltung des Postfachs ist technikoffen. Die Möglichkeit, mehrere Postfächer, insbesondere im Rahmen von Organisationskonten zu nutzen, ist nicht ausgeschlossen."

Nutzerkonten dienen der bidirektionalen Kommunikation zwischen Nutzern und Behörde. Dies setzt voraus, dass mit der Registrierung und Anlage eines Nutzerkontos auch ein Postfach als Komponente des Nutzerkontos bereitgestellt wird. Mit dieser Komponente wird eine Möglichkeit geschaffen dem Nutzer medienbruchfrei bezüglich einer Anfrage oder eines Antrags zu antworten.

Datenschutzerklärung

In der Datenschutzerklärung zum hamburgischen Servicekontos wird ausgeführt: "Die Daten werden nur für den Zweck verwendet, für den sie erhoben wurden. Eine Weitergabe erfolgt an die von Ihnen gewählten und tatsächlich genutzten Online-Dienste im Hamburg Serviceportal. Im Rahmen des Onlinezugangsgesetzes (OZG) ist es auch möglich, dass Sie Online-Verwaltungsdienste des Bundes oder anderer Bundesländer über das Hamburg Service-Portal beantragen."

Weiter wird dort erläutert: "Damit wir die gewünschten Leistungen für Sie erbringen können, ist es bei vielen Online-Diensten erforderlich, dass Sie Ihre Daten zur Verfügung stellen. Wir verarbeiten diese Daten nur im Rahmen Ihres Auftrags und verwenden sie nur unter Beachtung der gesetzlichen Bestimmungen (Onlinezugangsgesetz (OZG), Hamburgisches Datenschutzgesetz, EU Datenschutzgrundverordnung (DSGVO), Telekommunikationsgesetz, Telemediengesetz sowie einschlägige Fachgesetze wie beispielsweise das Meldegesetz)."

Die Ausführungen in der Datenschutzerklärung beinhalten zwar. (Bewertung von M1 eingefügen).....

Auftragsdatenverarbeitung

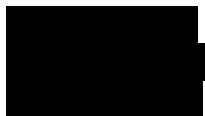
(Stand: Die Unterlagen sind bei der SK angefragt)

Dr. Sebastian Wirth

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichem Gruß

Dr. Sebastian Wirth



Bereich Technik und
Organisation

Datum: 7.12.2021

Bearbeiter: [REDACTED]

Telefon: [REDACTED]

Telefax: [REDACTED]

Zeichen: [REDACTED]/002/21/2036

(Zeichen bei Antwortschreiben bitte angeben)

Beschwerde nach Artikel 77 DS-GVO

- Sicherheit des Verwaltungsportals (#233296) – Ihre Anfrage bei „Frag den Staat“ vom 19. November 2021

Sehr geehrte [REDACTED],

wir bedanken uns nochmals für Ihre Anfrage nach Akteneinsichts- und Informationszugangsgesetz (AIG) / Beschwerde nach Artikel 77 Datenschutz-Grundverordnung (DS-GVO) zur Sicherheit des Verwaltungsportals (#233296), welche uns über die Plattform „Frag den Staat“ erreicht hat.

Vorliegend nehmen wir in Bezug auf Ihre o. g. Anfrage zu Ihrer Beschwerde nach Art. 77 DS-GVO Stellung, mit der Sie Zweifel äußern, dass die Verantwortlichen der Verwaltungsportale eine nach dem Stand der Technik entsprechende Sicherheit gewährleisten.

Zum Ersten verweisen Sie im Allgemeinen auf die von Ihnen angeführten Anfragen bei „Frag den Staat“ zur „Verschlüsselung und (Un-)Sicherheit der Verwaltungsportale“ und der „Verschlüsselung im BSI Grundschutz“. Zum Zweiten verweisen Sie hier auf Ihnen aufgefallene Mängel in Bezug auf die Verwendung von Sicherheitsfragen bzw. der Verpflichtung zum Postfach in Brandenburg Verwaltungsportalen.

Die hier von Ihnen extra angeführten Sicherheitsmängel (für Brandenburg) sind weder begründet, noch lässt sich aus Ihrer Darlegung ein konkreter Mangel bzw. ein Defizit herleiten. Ergänzend fehlen Ihrerseits Aussagen in Bezug auf Ihr Authentisierungsniveau in den jeweiligen Verwaltungsportalen, mit dem Sie sich registriert haben.

Die jeweiligen Authentisierungsmechanismen untersetzen jeweils ein entsprechendes Vertrauensniveau und bestimmen somit auch die Zulässigkeit bzw. Möglichkeit der Nutzung bestimmter Verwaltungsdienste im Verwaltungsportal; auch abhängig von Schutzbedarf der verarbeiteten personenbezogenen Daten und der rechtlich notwendigen eindeutigen Identitätsfeststellung des Betroffenen durch die verantwortliche Stelle.

Von: [Wirth, Sebastian Dr.](#)
An: [Wallbraun, Swantje](#)
Betreff: WG: [SPAMVERDACHT]Sicherheit des Verwaltungsportals [#233299]
Datum: Dienstag, 7. Dezember 2021 10:29:00

Az.: 3627_2021

Hallo Swantje,

wie gerade besprochen hier die Transparenzanfrage.
Sobald ich weiß, ob wir zum Verwaltungsportal Unterlagen haben, maile ich dir den Stand und ggf. den Inhalt.
Die den Aspekt der nicht ausreichenden TOMs und der Datenschutzerklärung des Verwaltungsportals der SK werde ich über die angegebene Mailadresse beantworten.

Gruß

Sebastian

--

Dr. Sebastian Wirth

Referat T

Referatsleiter für den technischen Datenschutz, T

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift:

Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsstelle:

Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

Durchwahl

Büro: +49 (0)40 428 54-4053

E-Mail

sebastian.wirth@datenschutz.hamburg.de

Webauftritt

datenschutz-hamburg.de

-----Ursprüngliche Nachricht-----

Von: Transparenzgesetz

Gesendet: Freitag, 19. November 2021 13:13

An: Mailbox (HmbBfDI) <mailbox@datenschutz.hamburg.de>

Betreff: WG: [SPAMVERDACHT]Sicherheit des Verwaltungsportals [#233299]

Von: Christina Franke [#233299]

Gesendet: Freitag, 19. November 2021 13:12:49 (UTC+01:00) Amsterdam, Berlin, Bern, Rom, Stockholm, Wien

An: Transparenzgesetz

Betreff: [SPAMVERDACHT]Sicherheit des Verwaltungsportals [#233299]

Hamburgischen Transparenzgesetz (HmbTG) / Beschwerde nach Artikel 77 DSGVO

Sehr geehrte Damen und Herren,

Ich muss anzweifeln, dass die Verantwortlichen der Verwaltungsportale ein dem Stand der Technik entsprechende Sicherheit gewährleisten und mich dementsprechend über die Verwaltungsportale beschweren.

Ich verweise auf <https://fragdenstaat.de/anfrage/verschlüsselung-un-sicherheit-der-verwaltungsportale/> und <https://fragdenstaat.de/anfrage/verschlüsselung-im-bsi-grundschutz/> und lege Beschwerde wegen Verstoß gegen Artikel 32 DSGVO ein.

Abgesehen von der aller Wahrscheinlichkeit nach fehlenden Verschlüsselung sind mir weitere Mängel aufgefallen, die ich ebenfalls in <https://fragdenstaat.de/anfrage/verschlüsselung-un-sicherheit-der-verwaltungsportale/> aufgezählt habe. Im Fall Hamburg sind das

- * eine abweichende Domäne zwischen Portal und gesendeten Emails,
- * die Verpflichtung zum Postfach.

Darüberhinaus halte ich die Datenschutzerklärung für fragwürdig, denn sie gibt die Rechtsgrundlagen der Datenverarbeitung nicht korrekt wieder.

Da meines Wissens Auftragsverarbeiter beauftragt sind, bitte ich Sie auch zu prüfen ob entsprechend Artikel 28 DSGVO entsprechende Verträge geschlossen wurden. Die widerwilligen Antworten auf die Anfragen von Frau Maier - https://fragdenstaat.de/anfragen/?user=v.maier_3 - lassen mich vermuten, dass Verträge fehlen oder keine Artikel 32 DSGVO - Stand der Technik - erfüllenden TOMs enthalten.

Ausschlussgründe liegen meines Erachtens nicht vor. Sofern Teile der Information durch Ausschlussgründe geschützt sind, beantrage ich mir die nicht geschützten Teile zugänglich zu machen.

Ich bitte Sie zu prüfen, ob Sie mir die erbetene Auskunft auf elektronischem Wege kostenfrei erteilen können. Sollte die Aktenauskunft Ihres Erachtens in jedem Fall gebührenpflichtig sein, möchte ich Sie bitten, mir dies vorab mitzuteilen und dabei die Höhe der Kosten anzugeben.

Ich verweise auf § 13 Abs. 1 HmbTG und bitte Sie, mir die erbetenen Informationen unverzüglich und nur im Ausnahmefall spätestens nach Ablauf eines Monats nach Antragszugang zugänglich zu machen.

Sollten Sie für diesen Antrag nicht zuständig sein, bitte ich Sie, ihn an die zuständige Behörde weiterzuleiten und mich darüber zu unterrichten. Ich widerspreche ausdrücklich der Weitergabe meiner Daten an Dritte.

Ich möchte Sie um eine Antwort in elektronischer Form (E-Mail) bitten und bitte Sie um eine Empfangsbestätigung. Danke für Ihre Mühe!

Mit freundlichen Grüßen
Christina Franke

Anfragenr: 233299
Antwort an: c.franke.6.zhufhf83u@fragdenstaat.de

Laden Sie große Dateien zu dieser Anfrage hier hoch:
<https://fragdenstaat.de/anfrage/233299/upload/06e680fa5f16aed3d7697fea7383b5a84e1dfdaa/>

Postanschrift
Christina Franke
Hirschstraße 152
76137 Karlsruhe

--

Rechtshinweis: Diese E-Mail wurde über den Webservice fragdenstaat.de versendet. Antworten werden ggf. im Auftrag der Antragstellenden auf dem Internet-Portal veröffentlicht.

Falls Sie Fragen dazu haben oder eine Idee, was für eine Anfrage bei Ihnen im Haus notwendig wäre, besuchen Sie:

<https://fragdenstaat.de/fuer-behoerden/>

Informationen zum Datenschutz nach der EU Datenschutz-Grundverordnung (DS-GVO)

Datenschutzerklärung

Nahezu alle Bürgerinnen und Bürger sowie Unternehmen treten mit der Verwaltung früher oder später in Kontakt, weil sie z.B. einen Personalausweis beantragen müssen oder Kindergeld beanspruchen können. Hierbei müssen personenbezogene Daten verarbeitet werden.

In einem Verwaltungsverfahren sind Daten personenbezogen, wenn sie einer natürlichen Person zugeordnet werden können. Keine personenbezogenen Daten sind anonymisierte Daten.

Wenn Verwaltungsbehörden personenbezogene Daten verarbeiten, bedeutet das, dass sie diese Daten z. B. erheben, speichern, verwenden, übermitteln, zum Abruf bereitstellen oder löschen.

Die Daten werden nur für den Zweck verwendet, für den sie erhoben wurden. Eine Weitergabe erfolgt an die von Ihnen gewählten und tatsächlich genutzten Online-Dienste im Hamburg Serviceportal. Im Rahmen des Onlinezugangsgesetzes (OZG) ist es auch möglich, dass Sie Online-Verwaltungsdienste des Bundes oder anderer Bundesländer über das Hamburg Service-Portal beantragen. Werden Dienste von Behörden erbracht, die nicht zur Freien und Hansestadt Hamburg gehören, übermitteln wir Ihre Daten an die für die beantragte Verwaltungsleistung zuständige Stelle. Wann das der Fall ist, schildern wir unter der Rubrik: „Unter welchen Voraussetzungen dürfen wir Ihre Daten an Dritte weitergeben“.

Im Folgenden informieren wir Sie darüber, welche personenbezogenen Daten wir erheben, bei wem wir sie erheben und was wir mit diesen Daten machen. Außerdem informieren wir Sie über Ihre Rechte in Datenschutzfragen und an wen Sie sich diesbezüglich wenden können.

Inhaltsverzeichnis

[Wer sind wir?](#)

[Wer sind Ihre Ansprechpartner?](#)

[Warum und zu welchem Zweck verarbeiten wir Ihre personenbezogenen Daten?](#)

[Welche personenbezogenen Daten verarbeiten wir?](#)

[Wie verarbeiten wir diese Daten?](#)

[Unter welchen Voraussetzungen dürfen wir Ihre Daten an Dritte weitergeben?](#)

[Wie lange speichern wir Ihre Daten?](#)

[Welche Rechte \(Auskunftsrecht, Widerspruchsrecht usw.\) haben Sie?](#)

Wer sind wir?

Das **Hamburg Serviceportal** der Freien und Hansestadt Hamburg bietet einen sicheren Zugang zu den Online-Diensten der Stadt. Es bietet Ihnen Funktionen, mit denen Sie Online-Dienstleistungen suchen und finden, sich für die Nutzung von Online-Diensten registrieren und anmelden sowie in Bezug auf genutzte Online-Dienste sicher mit der Verwaltung kommunizieren können.

Damit wir die gewünschten Leistungen für Sie erbringen können, ist es bei vielen Online-Diensten erforderlich, dass Sie Ihre Daten zur Verfügung stellen. Wir verarbeiten diese Daten nur im Rahmen Ihres Auftrags und verwenden sie nur unter Beachtung der gesetzlichen Bestimmungen (Onlinezugangsgesetz (OZG), Hamburgisches Datenschutzgesetz, EU Datenschutzgrundverordnung (DSGVO), Telekommunikationsgesetz, Telemediengesetz sowie einschlägige Fachgesetze wie beispielsweise das Meldegesetz).

Online-Dienste im Hamburg Serviceportal

Die untenstehenden Informationen beziehen sich auf das Hamburg Serviceportal, insbesondere auf die Benutzerkonten (Servicekonten) und Servicekonto-Postfächer. Informationen zu den einzelnen Online-Diensten finden Sie bei den [Informationen zum Datenschutz bei der Verwendung von Online-Diensten](#).

Wer sind Ihre Ansprechpartner?

Fragen in datenschutzrechtlichen Angelegenheiten können Sie an den für die Servicekonten und das Portal zuständigen Datenschutzbeauftragten der Senatskanzlei richten:

Senat der Freien und Hansestadt Hamburg
Datenschutzbeauftragter der Senatskanzlei
Hermannstraße 15, 20095 Hamburg
Tel.: +49 40 42831 – 2500
E-Mail: behoerdlicherdatenschutz@sk.hamburg.de

Falls Sie Fragen zur Registrierung oder Anmeldung haben oder uns Ihre Anregungen oder Hinweise zum Serviceportal mitteilen möchten, nehmen Sie bitte unter der E-Mail-Adresse meinserviceportal@dataport.de Kontakt zu uns auf.

Freie und Hansestadt Hamburg
Senatskanzlei
Amt für IT und Digitalisierung
Fachliche Leitstelle für den HamburgService / das Hamburg Serviceportal
Rathausmarkt 1, 20095 Hamburg
Telefon: +49 40 42823 – 2500
E-Mail: meinserviceportal@dataport.de

Warum und zu welchem Zweck verarbeiten wir Ihre personenbezogenen Daten?

Wir verarbeiten Ihre personenbezogenen Daten, damit Sie die über das Service-Portal angebotenen Verwaltungsleistungen online in Anspruch nehmen können (Verarbeitungszweck).

Im Hamburg Serviceportal werden Ihre Daten zunächst zur Einrichtung eines Benutzerkontos (Servicekonto) verarbeitet. Ein Servicekonto ist zur Nutzung der zur Verfügung gestellten Online-Dienste erforderlich. Wenn Sie dann Online-Dienste über Ihr Nutzerkonto beanspruchen, übermitteln

wir Ihre Daten an die zuständige Fachbehörde. Ihre einmalige Einwilligung ist grundlegend für die Verarbeitung Ihrer Daten für alle Online-Dienste der Stadt, die Sie aus Ihrem Nutzerkonto über das Service-Portal abwickeln möchten.

Im Rahmen des Online-Zugangsgesetzes liegt die Verantwortlichkeit für die Verarbeitung Ihrer Daten in bestimmten Fällen auch zusätzlich in anderen Bundesländern, an die Ihre Daten dann für die Nutzung eines solchen Online-Dienstes übermittelt werden. Vor einer Übermittlung fragen wir Ihre Einwilligung in jedem Einzelfall ab.

Zu jedem Servicekonto gehört ein Postfach, damit Sie im Zusammenhang mit der Nutzung von Online-Diensten sicher mit der Verwaltung kommunizieren können. Die Verarbeitung von Daten des Servicekonto-Postfachs erfolgt auf Basis Ihrer Einwilligung und aufgrund der Erfüllung rechtlicher Verpflichtungen sowie der einschlägigen Rechtsvorschriften der von Ihnen genutzten Online-Dienste. Auf das Postfach und die gespeicherten Nachrichten können nur Sie als Inhaber des Servicekontos nach einer Anmeldung am Servicekonto zugreifen. Welche personenbezogenen Daten in einer Postfachnachricht enthalten sind, hängt von der jeweiligen Nachricht und dem Online-Dienst ab, in dessen Zusammenhang die Nachricht verschickt wird.

Zur Gewährleistung der Funktionalität des Online-Dienstes ist es erforderlich, dass Ihre Daten an die jeweils zuständigen Behörden übermittelt werden und Sie dieser Übermittlung zugestimmt haben (Einwilligung). Der Zweck der Übermittlung Ihrer Daten besteht darin, dass Sie die von dem Onlinedienst angebotene Verwaltungsleistung in Anspruch nehmen können.

Sie sind nicht verpflichtet, diese Einwilligung zu erteilen. Sollten Sie Ihre Einwilligung nicht erteilen, erfolgt keine Übermittlung Ihrer Daten. Damit kann allerdings auch die von Ihnen begehrte Verwaltungsleistung über Ihr Nutzerkonto nicht in Anspruch genommen werden. Wenden Sie sich in diesem Fall direkt an die zuständige Behörde, Sie können die Verwaltungsleistung auch dort in nicht-elektronischer Weise in Anspruch nehmen.

Sie können Ihre Einwilligung jederzeit widerrufen. Dadurch wird allerdings die damit ausgelöste Übermittlung Ihrer Daten nicht rückgängig gemacht. Eine Löschung bzw. Sperrung Ihrer übermittelten Daten müssen Sie direkt bei der oben genannten verantwortlichen Stelle geltend machen.

Beispiele zur Verarbeitung:

Beispiel 1: Sie möchten einen Online-Dienst nutzen, der ein Servicekonto erfordert. Sie registrieren sich dazu im Serviceportal. Mit dem Abschluss der Registrierung besitzen Sie ein Servicekonto, in dem Daten zu Ihrer Person gespeichert sind (s. unten). Zu diesem Servicekonto gehört ein Postfach. Bei der Nutzung einiger Online-Dienste erhalten Sie z.B. eine Auskunft in Form einer Postfach-Nachricht in Ihr Postfach. Sie werden z.B. per E-Mail über den Eingang der Nachricht in ihr Postfach informiert. Um die Nachricht zu lesen, müssen Sie sich an Ihrem Servicekonto anmelden und in das Postfach navigieren.

Beispiel 2: Sie möchten einen Online-Dienst eines anderen Bundeslandes oder des Bundes nutzen. Sie können den Dienst online aufrufen und sich dann mit Ihrem Hamburger Servicekonto anmelden. Sobald Sie in die Übermittlung Ihrer Daten eingewilligt haben, werden die personenbezogenen Daten aus Ihrem Nutzerkonto an die verantwortliche Stelle des anderen Bundeslandes oder des Bundes übermittelt, die für den Betrieb des von Ihnen aufgerufenen Dienstes datenschutzrechtlich verantwortlich ist.

Welche personenbezogenen Daten verarbeiten wir?

Wir verarbeiten insbesondere folgende personenbezogene Daten:

Einfaches Servicekonto für Bürgerinnen und Bürger („Servicekonto“)

Für die Nutzung von Online-Diensten mit dem Kontotyp einfaches „Servicekonto“ speichern wir nach Ihrer Zustimmung folgende personenbezogene Daten:

1. Vorname
2. Nachname
3. E-Mail-Adresse
4. Passwort
5. Wahl der Darstellungssprache (derzeit immer „Deutsch“)
6. Servicekontotyp (freigeschaltete Sicherheitsstufe)
7. Datum der Einwilligung zur Datenverarbeitung

Servicekonto mit Identifikationsnachweis für Bürgerinnen und Bürger („Servicekonto Plus“)

Für die Nutzung von Online-Diensten mit dem Kontotyp „Servicekonto Plus“ speichern wir nach Ihrer Zustimmung folgende personenbezogene Daten:

1. Vorname
2. Nachname
3. Adresse (Straße, Hausnummer, PLZ, Ort, Land)
4. Geburtsdatum
5. Geburtsname
6. Geburtsort
7. E-Mail-Adresse
8. Passwort
9. Wahl der Darstellungssprache (derzeit immer „Deutsch“)
10. Servicekontotyp (freigeschaltete Sicherheitsstufe)
11. Datum der Einwilligung zur Datenverarbeitung

Daten, die Sie als Bürgerin oder Bürger zusätzlich angeben können

Sie haben die Möglichkeit, weitere Daten in Ihrem Servicekonto zu hinterlegen. Diese Daten werden in manchen Online-Diensten dazu verwendet, Felder in Formularen vorauszufüllen, um Ihnen die Eingabe zu ersparen.

Wenn Sie ein einfaches Servicekonto besitzen („Servicekonto“), können Sie optional auch die Daten für das „Servicekonto Plus“ ausfüllen (s. oben).

Sowohl für das „Servicekonto“ als auch das „Servicekonto Plus“ können Sie folgende Daten zusätzlich angeben:

1. Anrede
2. Akademischer Titel
3. Adresszusatz
4. Telefonnummer
5. Mobiltelefonnummer

Hinterlegung Ihrer Zahlungsdaten beim Payment Provider zur Wiederverwendung bei Zahlungsvorgängen mit ePayment

Bei Online-Dienstleistungen, die Sie online per ePayment bezahlen können, haben Sie die Möglichkeit, die einmal angegebenen Zahlungsdaten (z.B. Ihre Kontodaten) beim Payment Provider speichern zu lassen. In diesem Fall wird in Ihrem Servicekonto eine Referenznummer des Payment

Providers gespeichert. Die beim Payment Provider gespeicherten Daten können Sie bei späteren Zahlungsvorgängen wiederverwenden, sodass Sie die Daten nicht erneut eingeben müssen.

Ab 2021 erfolgt ein Umstieg auf die von der Entwicklergemeinschaft Bund-Länder entwickelte Zahlungskomponente ePayBL. Bei dieser Zahlkomponente werden die Zahlungsdaten nicht beim Payment Provider hinterlegt.

Registrierung eines Servicekontos für Bürgerinnen und Bürger mithilfe der eID-Funktion des Personalausweises

Wenn Sie sich mit der eID-Funktion des Personalausweis registrieren, werden die Daten Nr. 1-6 vom Personalausweis ausgelesen und gespeichert, sofern Sie dem zugestimmt haben.

Zusätzlich wird das "Pseudonym" bzw. „Kartenkennung" Ihres Ausweises gespeichert, wenn Sie die Funktion "Anmelden mit Online-AusweisFunction" aktiviert haben.

Servicekonto für Unternehmen und andere Organisationen („Servicekonto Business“)

Bei Servicekonten für Unternehmen, Behörden und andere Organisationen sind unterschiedliche Daten zu unterscheiden: 1. Daten zum Unternehmen, 2. Daten zu Administratoren für das „Servicekonto Business“ und 3. Daten zu Mitarbeiterinnen und Mitarbeitern, die Online-Dienste nutzen.

Zum Unternehmen / zur Organisation

Folgende Daten werden zu Organisationen gespeichert:

1. Name der Organisation
2. Organisationsadresse (Straße, Hausnummer, PLZ, Ort, Land)
3. Freigeschaltete Online-Dienste
4. Nutzung von Online-Diensten durch die Administratoren

Zum Servicekonto-Administrator für das „Servicekonto Business“

Administratoren für ein „Servicekonto Business“ sind Nutzer im Unternehmen, die erweiterte Berechtigungen auf ein „Servicekonto Business“ besitzen und neben ihren eigenen Daten auch die Daten zum Unternehmen bzw. der Organisation ändern können. Sie können außerdem die Mitarbeiterinnen und Mitarbeiter des Unternehmens verwalten (einrichten, löschen, ändern und technisch berechtigen), die für das Unternehmen Online-Dienste nutzen. Zu Administratoren werden folgende Daten gespeichert:

1. Vorname
2. Nachname
3. E-Mail-Adresse
4. Passwort
5. Telefonnummer
6. Wahl der Darstellungssprache (derzeit immer „Deutsch“)
7. Servicekontotyp
8. Datum der Einwilligung zur Datenverarbeitung
9. Berechtigungsrollen in Online-Diensten

Zu Unternehmens- bzw. Organisationsmitarbeiterinnen und -mitarbeitern eines „Servicekonto Business“

Mitarbeiterinnen und Mitarbeiter des Unternehmens oder der Organisation werden vom Servicekonto-Administrator (s. oben) eingerichtet und verwaltet. Sie werden durch den Servicekonto-Administrator zur Nutzung von Online-Diensten im Namen des Unternehmens oder der Organisation technisch berechtigt. Zu Unternehmens- bzw. Organisationsmitarbeitern werden folgende Daten gespeichert:

1. Vorname
2. Nachname
3. E-Mail-Adresse
4. Passwort
5. Wahl der Darstellungssprache (derzeit immer „Deutsch“)
6. Servicekontotyp

Daten, die Sie für „Servicekonto Business“-Nutzer zusätzlich angeben können

Sie haben die Möglichkeit, weitere Daten in Ihrem „Servicekonto Business“ zu hinterlegen. Diese Daten werden in manchen Online-Diensten dazu verwendet, Felder in Formularen vorauszufüllen, um Ihnen die Eingabe zu ersparen:

1. Anrede
2. Akademischer Titel (zu Administratoren und Mitarbeiter/innen)
3. Organisationseinheit (zu Administratoren und Mitarbeiter/innen)
4. Faxnummer (bei Organisations-Administratoren)
5. Telefonnummer (bei Mitarbeiter/innen)
6. Mobiltelefonnummer (bei Administratoren und bei Mitarbeiter/innen)
7. Handelsregisternummer (zur Organisation)
8. E-Mail-Adresse der Organisation
9. Postfach-Nummer der Organisation
10. Postfach-PLZ der Organisation

Hinterlegung Ihrer Zahlungsdaten beim Payment Provider zur Wiederverwendung bei Zahlungsvorgängen mit ePayment

Sie haben die Möglichkeit, die einmal angegebenen Zahlungsdaten (z.B. Ihre Kontodaten) beim Payment Provider speichern zu lassen. In diesem Fall wird in Ihrem „Servicekonto Business“ eine Referenznummer des Payment Providers gespeichert. Die beim Payment Provider gespeicherten Daten können Sie bei späteren Zahlungsvorgängen wiederverwenden, sodass Sie die Daten nicht erneut eingeben müssen.

Ab 2021 erfolgt ein Umstieg auf die von der Entwicklergemeinschaft Bund-Länder entwickelte Zahlungskomponente ePayBL. Bei dieser Zahlkomponente werden die Zahlungsdaten nicht beim Payment Provider hinterlegt.

Wichtiger Hinweis zum Passwort

Halten Sie Ihr Passwort geheim, damit keine unberechtigten Personen Zugang zu Ihren Daten erlangen. Geben Sie Ihr Passwort nicht auf Nachfrage bekannt. Auch die technischen Betreuer des Hamburg Serviceportals sind nicht berechtigt, Ihr Passwort zu erfahren.

Servicekonto-Postfach

Wenn Sie ein Servicekonto nutzen, wird für Sie auch ein Servicekonto-Postfach angelegt. Für die Nutzung werden folgende Daten aus dem Servicekonto im Postfach-System gespeichert:

- Anrede
- Vorname

- Nachname
- E-Mail-Adresse
- Telefonnummer

Daneben werden innerhalb des Servicekonto-Postfachs die Nachrichtenkonversation zwischen Ihnen und den Behörden gespeichert. In den Nachrichten können personenbezogene Daten enthalten sein, dies ist abhängig davon, welche Verwaltungsleistung Sie nutzen.

Suchen & Finden des Online-Gateways Portalverbund

Wenn Sie im Suchfeld eine andere Stadt als Hamburg eingeben, wird die Suche durch das Online-Gateway Portalverbund ausgeführt. Mit dem Online-Gateway können Sie deutschlandweit nach Verwaltungsleistungen suchen. Die von Ihnen als Bürgerin oder Bürger während der Suche verarbeiteten Daten werden nicht gespeichert und nicht weiterverarbeitet. Der Zugriff auf die Suchfunktion erfolgt pseudonym. Es wird keine Suchhistorie und auch keine Historie der Vervollständigung der Begriffe erstellt. Es erfolgt keine Verknüpfung mit Ihren bestehenden Benutzerkonten aus den Verwaltungsportalen (Servicekonten).

Ihre IP-Adresse und der verwendete Internet-Browser werden in technischen Protokollen (Logfiles) erfasst. Die Notwendigkeit der Speicherung dieser Daten ergibt sich aus den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik. Dabei erfolgt im Regelfall eine Speicherung für drei Tage. Bei Auffälligkeiten der Aufrufe werden die Daten zur Analyse für maximal 1 Jahr sicher aufbewahrt.

Wie verarbeiten wir diese Daten?

Ihre personenbezogenen Daten werden gespeichert. Sofern Sie an Ihrem Servicekonto angemeldet sind, werden die Daten aus Ihrem Servicekonto in bestimmten Online-Diensten dazu genutzt, Formularfelder vorauszufüllen, so dass Sie diese Daten nicht erneut eingeben müssen. Erst wenn Sie eine explizite Aktion wie z.B. das Senden eines von Ihnen ausgefüllten Online-Formulars (i.d.R durch einen Klick auf eine entsprechend bezeichnete Schaltfläche) ausführen, werden diese Daten in das dem Online-Dienst zugeordnete Verwaltungsverfahren übernommen.

Wir setzen technische und organisatorische Sicherheitsmaßnahmen ein, um Ihre personenbezogenen Daten gegen unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust oder Veränderung sowie gegen unbefugte Offenlegung oder unbefugten Zugang zu schützen. Unsere Sicherheitsstandards entsprechen stets den aktuellsten technologischen Entwicklungen.

Unter welchen Voraussetzungen dürfen wir Ihre Daten an Dritte weitergeben?

Alle personenbezogenen Daten, die uns in einem Verwaltungsverfahren bekannt geworden sind, dürfen wir nur dann an andere Personen oder Stellen weitergeben, wenn Sie der Weitergabe zugestimmt haben oder die Weitergabe gesetzlich zugelassen ist.

Werden Dienste von Behörden erbracht, die nicht zur Freien und Hansestadt Hamburg gehören, so wird Ihnen dies deutlich angezeigt. Bund und Länder haben sich nach dem Onlinezugangsgesetz (OZG) zusammengeschlossen, um den Bürgern elektronisch Verwaltungsleistungen anbieten zu können. Mit Ihrem Hamburger Benutzerkonto können Sie die Leistungen andere Portale des Bundes und der Länder nutzen. In einem solchen Fall werden Ihre Daten an die bearbeitende Stelle weitergegeben. Sie werden im Einzelfall vor einer solchen Weitergabe informiert und müssen ihr auch zustimmen.

Damit Sie Online-Dienste eines anderen Bundeslandes oder des Bundes mit Ihrem Konto nutzen können, haben die Verantwortlichen für die Nutzerkonten der Bundesländer und des Bundes gemeinsame Vorgehensweisen, Datenflüsse und die Festlegung von technischen Anforderungen in einer Verwaltungsvereinbarung festgeschrieben. Diese regelt auch die Verantwortlichkeiten bei der Verarbeitung Ihrer personenbezogenen Daten, wenn Sie Online-Dienste anderer Bundesländer mit Ihrem Nutzerkonto nutzen. Es ist somit nicht erforderlich, dass Sie in dem anderen Bundesland bzw. beim Bund ein zusätzliches Nutzerkonto anlegen. Näheres erfahren Sie [hier](#).

Eine Datenübermittlung an Dritte findet auch beim ePayment statt. Das Rechenzentrum des derzeitigen Payment-Providers „SIX Payment Services (Germany) GmbH“ befindet sich in der Schweiz. Das Datenschutzniveau in der Schweiz wurde von der EU als gleichwertig anerkannt. Je nach Online-Dienstleistung können im Verwendungszweck des Zahlungsvorgangs personenbezogene Daten übertragen werden (z.B. ein Aktenzeichen oder andere fachliche Referenznummer).

Ab 2021 erfolgt ein Umstieg auf die von der Entwicklergemeinschaft Bund-Länder entwickelte Zahlungskomponente ePayBL. Das Hosting von ePayBL erfolgt durch den SID (Staatsbetrieb Sächsische Informatik Dienste), die ihre Rechenzentren PCI-DSS-konform betreiben und entsprechend der Sensibilität der vorliegenden Daten unter Berücksichtigung hoher Datenschutzauflagen handeln. Der Payment Provider ist dann PAYONE Girosolution. Der Payment Provider unterliegt der Regulierung des Bankengeschäfts und den damit verbundenen Sicherheitsstandards.

Wie lange speichern wir Ihre Daten?

Servicekonto

Wir speichern Ihre Daten in Ihrem Servicekonto, solange Sie es nutzen. Wenn Sie Ihr Servicekonto eine festgelegte Zeit lang nicht nutzen, wird es gelöscht: Im Fall des „Servicekonto Plus“ und „Servicekonto Business“ beträgt der Zeitraum fünf Jahre, im Fall einfacherer Servicekonten zwei Jahre. Vor der endgültigen Löschung weist das System Sie per E-Mail darauf hin, dass Ihr Servicekonto inklusive Postfach und aller enthaltenen Postfach-Nachrichten gelöscht werden wird, sofern Sie sich nicht erneut am Servicekonto anmelden.

Servicekonto-Postfach

Die Postfachnachrichten werden gespeichert, bis sie gelöscht werden. Die Löschung erfolgt ausschließlich durch Sie. Eine automatische Löschung der Postfachnachrichten erfolgt nicht, allerdings werden alle Postfachnachrichten gelöscht, wenn das zugrundeliegende Servicekonto gelöscht wird.

Welche Rechte (Auskunftsrecht, Widerspruchsrecht usw.) haben Sie?

Sie haben nach der Datenschutz-Grundverordnung verschiedene Rechte. Einzelheiten ergeben sich insbesondere aus Artikel 15 bis 18 und 21 der Datenschutz-Grundverordnung.

Recht auf Auskunft

Sie können Auskunft über Ihre von uns verarbeiteten personenbezogenen Daten verlangen. In Ihrem Auskunftsantrag sollten Sie Ihr Anliegen präzisieren, um uns das Zusammenstellen der erforderlichen Daten zu erleichtern. Daher sollten in dem Antrag möglichst Angaben zum konkreten Verwaltungsverfahren und zum Verfahrensabschnitt gemacht werden.

Recht auf Berichtigung

Sollten die Sie betreffenden Angaben nicht (mehr) zutreffend sein, können Sie eine Berichtigung verlangen. Sollten Ihre Daten unvollständig sein, können Sie eine Vervollständigung verlangen.

Recht auf Löschung

Sie können die Löschung Ihrer personenbezogenen Daten verlangen. Ihr Anspruch auf Löschung hängt u. a. davon ab, ob die Sie betreffenden Daten von uns zur Erfüllung unserer gesetzlichen Aufgaben noch benötigt werden.

Die Löschung Ihrer Daten erfolgt in diesem Fall unverzüglich.

Recht auf Einschränkung der Verarbeitung

Sie haben das Recht, eine Einschränkung der Verarbeitung der Sie betreffenden Daten zu verlangen. Die Einschränkung steht einer Verarbeitung nicht entgegen, soweit an der Verarbeitung ein wichtiges öffentliches Interesse besteht.

Recht auf Widerspruch

Sofern Ihre Daten nicht auf der Grundlage Ihrer Einwilligung, sondern aus Gründen eines überwiegenden öffentlichen Interesses oder einer Rechtsvorschrift verarbeitet werden, haben Sie das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit der Verarbeitung der Sie betreffenden Daten zu widersprechen.

Recht auf Beschwerde

Wenn Sie der Auffassung sind, dass wir Ihrem Anliegen nicht oder nicht in vollem Umfang nachgekommen sind, können Sie bei der zuständigen Datenschutzaufsichtsbehörde Beschwerde einlegen:

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str 22, 7. OG, 20459 Hamburg
Tel.: (040) 4 28 54 - 40 40
E-Fax: (040) 4 279 – 11811
E-Mail: mailbox@datenschutz.hamburg.de

Allgemeine Hinweise zu diesen Rechten

In einigen Fällen können oder dürfen wir Ihrem Anliegen nicht entsprechen. Sofern dies gesetzlich zulässig ist, teilen wir Ihnen in diesem Fall immer den Grund für die Verweigerung mit.

Wir werden Ihnen aber grundsätzlich innerhalb eines Monats nach Eingang Ihres Anliegens antworten. Sollten wir länger als einen Monat für eine abschließende Klärung brauchen, erhalten Sie eine Zwischennachricht.

Informationen zu Cookies und Messverfahren zur Nutzung des Hamburg Serviceportals

Cookies

Cookies sind Datenelemente, die eine Website an Ihren Browser schickt, um sie auf Ihrem System zu speichern. Wir benutzen technisch notwendige "Sitzungs-Cookies", um Informationen aus der Website an Ihre Bedürfnisse anpassen zu können. Sobald Sie sich abmelden, werden die Cookies gelöscht.

Die meisten Browser können Sie so einstellen, dass Sie benachrichtigt werden, wenn Sie Cookies erhalten. Sie können dann selbst entscheiden, ob Sie das akzeptieren wollen oder nicht. Um den HamburgService nutzen zu können, müssen Sie diese Sitzungs-Cookies zulassen.

Stand 5. Mai 2021



BfDI

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Nur elektronisch:

[REDACTED]

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn

FON (0228) 997799-[REDACTED]

E-MAIL referat11@bfdi.bund.de

BEARBEITET VON [REDACTED]

INTERNET www.bfdi.bund.de

DATUM Bonn, 16.11.2021

GESCHÄFTSZ. 11-103 II#7156

**Bitte geben Sie das vorstehende Geschäftszeichen
bei allen Antwortschreiben unbedingt an.**

BETREFF **Ihre Anfrage beim BfDI über FragenStaat**

HIER Verschlüsselung und Sicherheit der Verwaltungsportale

Sehr geehrte(r) [REDACTED]

vielen Dank für Ihre Eingabe beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). In Ihrer Eingabe bewerten Sie einige technische Entscheidungen bei der Ausgestaltung des Nutzerkontos Bund (NKB) kritisch und fragen, ob diese Ausgestaltung mit den Anforderungen der DSGVO und des BDSG vereinbar sei. Insbesondere kritisieren Sie die Nutzung (vorformulierter) Sicherheitsfragen als Teil des Authentifizierungskonzeptes, den Rückgriff auf eine andere Domain beim Versenden von E-Mails als bei der Anmeldung ins NKB selbst sowie die nichtoptionale Ausgestaltung der Postfacheinrichtung. Daneben erwähnten Sie noch die Benennung der Rechtsgrundlagen in der Datenschutzerklärung des NKB.

Weiterhin kritisieren Sie einige technische und rechtliche Entscheidungen bei der Einrichtung diverser Nutzerkonten der Länder. Hier will ich allerdings vorab darauf hinweisen, dass ich insofern nicht für Ihre Anliegen zuständig bin, sondern allein die jeweiligen Datenschutzaufsichtsbehörden der Länder. Dem BfDI liegen hierzu ohnehin keine belastbaren eigenen Erkenntnisse vor.

Zu Ihren Kritikpunkten:

1. (Vorformulierte) Sicherheitsfragen

Es ist zutreffend, dass auch das NKB vorformulierte Sicherheitsfragen verwendet. Nach Ansicht des BfDI handelt es sich dabei jedoch nicht um ein Unterschreiten des gemäß Art. 32 DSGVO für die Verarbeitung personenbezogener Daten zwingend notwendigen Stands der Technik. Der Stand der Technik ist kein einheitlicher Anforderungskatalog, sondern bemisst sich nach dem jeweiligen Verarbeitungsszenario. Verarbeitungsszenario ist hier allein eine Hilfsfunktion im ohnehin niedrigsten Vertrauensniveau des NKB. Da schon zum Anlegen dieser (im niedrigsten Vertrauensniveau angesiedelten) Basisregistrierung allein der Zugang zum E-Mail-Account ausreicht und dort dem Stand der Technik entspricht, gilt dies auch für die ähnlich konstruierte Sicherheitsfrage, die damit verknüpft ist. Ein zusätzliches Sicherheitsmerkmal darüber hinaus würde die Anforderungen an das niedrigste(!) Vertrauensniveau bereits verlassen und in höhere Sphären vordringen.

2. Domainabweichung

Es ist zutreffend, dass auch das NKB beim Versenden von E-Mails auf eine andere Domain zurückgreift, als die Anmeldung beim NKB selbst. Nach Ansicht des BfDI handelt es sich dabei jedoch nicht um ein Unterschreiten des Stands der Technik im Sinne des Art. 32 DSGVO. Die Abweichung findet allein auf der Third-Level-Domain statt (Anmeldebestätigung: bmi.bund.de vs. NKB-Anmeldung: id.bund.de). Ein Sicherheitsrisiko, das den Stand der Technik unterschreitet, ist bei gleichbleibender Second-Level-Domain nicht erkennbar / etabliert.

3. Postfach im NKB

Es ist zutreffend, dass das Postfach des NKB sofort nach der Registrierung vorhanden ist. Nach Ansicht des BfDI handelt es dabei ebenfalls nicht um ein Unterschreiten des Stands der Technik im Sinne des Art. 32 DSGVO. Vielmehr stellt dies ein übliches Verhalten dar bei solchen Systemen. Auch steht diese Eigenschaft nicht im Widerspruch zu den rechtlichen Anforderungen gemäß § 2 Abs. 7 OZG. Danach ist das Postfach Bestandteil des Nutzerkontos, aber die Nutzung dessen ist freiwillig. Die gesetzliche Regelung sieht die Einrichtung des Postfachs an sich also gerade als unabhängig vom eigentlichen Nutzungswillen an.

4. Datenschutzerklärung des NKB

Es ist zutreffend, dass sich das NKB in seiner Datenschutzerklärung auf Art. 6 Abs. 1 lit. e) DSGVO in Verbindung mit den jeweils hauptsächlich einschlägigen Normen des OZG selbst beruft. Nach Ansicht des BfDI ist dieses Vorgehen korrekt und kein Verstoß gegen Art. 13, 14 DSGVO. Art. 6 Abs. 1 lit. e) DSGVO dient der Rechtfertigung der Verarbeitung personenbezogener Daten für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Allgemein wird diese Variante als einschlägig angesehen für die Verarbeitung insbesondere durch öffentliche Stellen in Erfüllung ihres gesetzlichen Auftrags. Der Bund / Das BMI haben durch die (ebenfalls mitzitierten) Regelungen des OZG den gesetzlichen Auftrag ein Nutzerkonto zu betreiben. Jedwede Datenverarbeitungen, die also hierfür notwendig sind, sind gleichzeitig notwendig für die Erfüllung des gesetzlichen Auftrags und können so über Art. 6 Abs. 1 lit. e) DSGVO rechtfertigt werden.

Ihre Vermutung, dass Art. 6 Abs. 1 lit. c) DSGVO einschlägig sein sollte, ist insofern unzutreffend. Gemäß Art. 6 Abs. 1 lit. c) DSGVO sind Verarbeitungen auch dann rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind, die der Verantwortliche unterliegt. Zielrichtung dieses Rechtfertigungsgrunds ist aber weniger der Staat selbst, sondern eher private Verantwortliche, die von einer staatlichen Auflage betroffen sind (ein zeitgerechtes Beispiel wäre wohl das Anfertigen von Gästelisten beim Zugang zu einem Restaurant o. ä. durch den Betreiber, weil eine Coronaschutzverordnung des jeweiligen Landes dies zwingend vorschreibt).

Wie von Ihnen zutreffend angemerkt, sollte die Rechtsgrundlage der Einwilligung gemäß Art. 6 Abs. 1 lit. a) DSGVO bei den eigentlichen Hauptleistungen des Nutzerkontos keine Rolle spielen.

Ich hoffe, dass ich Ihnen damit weiterhelfen konnte. Sollten Sie noch Fragen in der Sache haben, können Sie sich gerne wieder an mich wenden.

Mit freundlichen Grüßen
Im Auftrag

██████████

Von: [Wagner, Felix](#)
An: [Weber, Katja](#)
Cc: [Kühn, Ulrich](#)
Betreff: Rechtsgrundlage in der Datenschutzerklärung
Datum: Freitag, 21. Januar 2022 12:23:00
Anlagen: [DatenschutzerklärungRechtsgrundlage.pdf](#)

Moin Katja,

wie in der FBR besprochen sollte ich ja etwas für die Referatsleiterrunde schreiben, damit sich dort abgestimmt werden kann. Du hattest einen Dreizeiler vorgeschlagen – ich habe jetzt einen Zweiseiter gemacht. Damit etwas Kontext zur Verfügung steht. Wenn das für die RLR unangemessen ist, kann ich aber noch etwas Knapperes formulieren.

Gruß,

Felix

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de

Website: [datenschutz-hamburg.de](https://www.datenschutz-hamburg.de)

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.



Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Vermerk zu Az. 3672/2021 zur Vorlage in der Referatsleiterrunde

Prägnante Fragestellung:

Welche Anforderungen stellt der HmbBfDI an die Benennung der Rechtsgrundlagen in Datenschutzerklärungen (Art. 13 (1) c) bzw. Art. 14 (1) c) DSGVO)?

Hintergrund:

Die Beschwerde zum genannten Az. betrifft das hamburgische Serviceportal für Onlinedienste der Verwaltung (<https://serviceportal.hamburg.de>). Als Teilaspekt wird die Nennung der Rechtsgrundlagen in der Datenschutzerklärung kritisiert. Diese führt zu den Rechtsgrundlagen an:

Wir verarbeiten diese Daten nur im Rahmen Ihres Auftrags und verwenden sie nur unter Beachtung der gesetzlichen Bestimmungen (Onlinezugangsgesetz (OZG), Hamburgisches Datenschutzgesetz, EU Datenschutzgrundverordnung (DSGVO), Telekommunikationsgesetz, Telemediengesetz sowie einschlägige Fachgesetze wie beispielsweise das Meldegesetz).

Die Darstellung erscheint defizitär, da sehr pauschale Gesetzesverweise stattfinden. So dürfte die zentralste Norm für die Verarbeitung Art. 6 Abs. 1 e) DSGVO sein, in Verbindung mit jeweiligen Ermächtigungsvorschriften. Zumindest diese sollte benannt werden. Jedoch könnte eine vollständige, bis ins Detail erarbeitete Benennung aller Normen aufgrund der Vielzahl an Verwaltungsdienstleistungen sehr umfangreich sein. Es erscheint geboten, dass der HmbBfDI zunächst intern abstimmt, welchen Anforderungen eine Aufzählung der Rechtsnormen in Datenschutzerklärungen zu genügen hat, bevor Kontakt mit der Senatskanzlei aufgenommen wird.

Literatur:

Das Meinungsspektrum in der Kommentarliteratur geht zu der Frage auseinander. Beispielhaft seien hier zwei Extreme genannt:

Der Verantwortliche muss die betroffene Person zudem über die Rechtsgrundlage der Datenverarbeitung informieren. Nach dem Wortlaut der Norm reichte es hierzu aus, den einschlägigen Erlaubnistatbestand aus Art. 6 Abs. 1 und – in den Fällen der Art. 6 Abs. 1 lit. c und e – das hierzu nach

Art. 6 Abs. 2 und 3 ergangene mitgliedstaatliche oder Unionsrecht lediglich zu zitieren oder wörtlich zu wiederholen. Dies ermöglichte der betroffenen Person jedoch in manchen Fällen nicht, ihre rechtliche Position gegenüber der Datenverarbeitung einzuschätzen. Denn zum einen sind die Erlaubnistatbestände in Art. 6 Abs. 1 durchweg sehr offen formuliert. Zum anderen kann das Zusammenwirken von Art. 6 Abs. 1 lit. c und e mit den hierzu ergangenen Rechtsvorschriften komplexe Zuordnungsfragen aufwerfen. Die Informationspflicht ist darum weiter zu verstehen, damit sie ihren Zweck erfüllt. Der Verantwortliche muss der betroffenen Person in Fällen, in denen es wegen der Komplexität der Rechtslage oder aufgrund der erkennbaren Eigenschaften und Kenntnisse der betroffenen Person geboten ist, die Rechtslage **einzelfallbezogen und vollständig** darlegen. Dazu muss der Verantwortliche die Rechtsgrundlage der Datenverarbeitung so darstellen, dass die betroffene Person deren Anwendung auf ihren Fall nachvollziehen kann. [...]

(Bäcker, in: Kühling/Buchner, DS-GVO BDSG, 3. Aufl. 2020, Art. 13 DSGVO Rn. 26)

Die Pflicht zur Angabe der Rechtsgrundlage wurde im gemeinsamen Standpunkt des Rats v. 15.6.2015 eingeführt. Der Zweck ist klar: Der Betroffene soll selbst nachprüfen können, ob die Datenverarbeitung rechtmäßig ist. Demgegenüber sind bereits jetzt die praktischen Schwierigkeiten absehbar, da die Rechtsgrundlage oftmals nicht eindeutig angegeben werden kann, falls sich eine Datenverarbeitung unter mehrere Rechtsgrundlagen subsumieren lässt. Auch ist zB unklar, wie zu verfahren ist, wenn der Verantwortliche eine Rechtsgrundlage angibt, auf Basis derer er die Datenverarbeitung durchführt, die aber im Gegensatz zu einer anderen Rechtsgrundlage nicht zur Legitimation der Datenverarbeitung einschlägig ist oder sofern mehrere Rechtsgrundlagen einschlägig sind (→ Rn. 46.1 f.). Eine Literaturansicht (Schaffland/Wiltfang Art. 13 Rn. 11) ist der Meinung, dass die Angabe einer konkreten Rechtsgrundlage nur für öffentliche Stellen erforderlich sei und nichtöffentliche Stellen die Pflicht aus lit. c durch die Angabe „zum Anschluss und zur Durchführung des Vertrags“ erfüllen könnten. Ob dies der Fall ist, ist zweifelhaft, denn dies widerspricht dem Wortlaut und dem Sinn und Zweck der Vorschrift. Deutlich überzogen dürfte aber die Ansicht sein, dass der Verantwortliche dem Betroffenen die einschlägige Rechtsgrundlage einzelfallbezogen und vollständig die Subsumtion des Sachverhalts unter die einschlägige Rechtsgrundlage darzulegen hat (so aber Kühling/Buchner/Bäcker Art. 13 Rn. 26); eine derartige Darlegungspflicht ist abzulehnen, denn (1) sie ginge weit über den Wortlaut der Norm hinaus, (2) würde den Verantwortlichen letztlich dazu zwingen, vor jeder Information einen Rechtsanwalt hinzuzuziehen, (3) würde das "Subsumtionsrisiko" gänzlich auf den Verantwortlichen verlagern und (4) verstieße gegen die in Art. 16, 17 GRCh garantierten Rechte des Verantwortlichen (im Ergebnis auch Ehmann/Selmayr/Knyrim Art. 13 Rn. 27) (→ Rn. 46.1).

(Schmidt-Wudy, in: BeckOK Datenschutzrecht, Wolff/Brink, 38. Ed. St.: 01.11.2021, Art. 14 Rn. 46)

Von: [Wagner, Felix](#)
An: [REDACTED]
Cc: [Wirth, Sebastian Dr.](#); [REDACTED]
Betreff: Hamburg Serviceportal, Az. 3627/2021
Datum: Freitag, 11. Februar 2022 17:43:00

Sehr geehrte Frau [REDACTED],
sehr geehrte Damen und Herren,

Der HmbBfDI hat eine Beschwerde über das Hamburg ServicePortal erhalten (<https://serviceportal.hamburg.de/>). Die Beschwerde betrifft weitestgehend Einzelheiten, die der HmbBfDI nicht als datenschutzrechtlich problematisch beurteilt. Einer der Beschwerdegegenstände bezieht sich auf die Nennung der Rechtsgrundlage in der zugehörigen Datenschutzerklärung (<https://serviceportal.hamburg.de/HamburgGateway/FVP/FV/BasisHilfe/Datenschutz.aspx>). Dort heißt es:

„Wir verarbeiten diese Daten nur im Rahmen Ihres Auftrags und verwenden sie nur unter Beachtung der gesetzlichen Bestimmungen (Onlinezugangsgesetz (OZG), Hamburgisches Datenschutzgesetz, EU Datenschutzgrundverordnung (DSGVO), Telekommunikationsgesetz, Telemediengesetz sowie einschlägige Fachgesetze wie beispielsweise das Meldegesetz).“

Der HmbBfDI stimmt der Beschwerde insoweit zu, dass diese sehr pauschale Formulierung wohl nicht die Informationspflicht gem. Art. 13 Abs. 1 c) DSGVO erfüllt. Die Nennung der Rechtsgrundlage soll betroffene Personen in die Lage versetzen, eine belastbare Prüfung der zugrunde gelegten Rechtsnormen vorzunehmen (vgl. *Paal/Hennemann*, in: Paal/Paaly, DS-GVO BDSG, 3. Aufl. 2021, Art. 13 DSGVO, Rn. 16a).

Der HmbBfDI geht davon aus, dass der Ausgangspunkt der Verarbeitung stets Art. 6 Abs. 1 e) DSGVO sein dürfte, in Verbindung mit den jeweiligen Fachgesetzen. Aus Sicht des HmbBfDI muss die Benennung der Rechtsgrundlage zwar nicht jeden denkbaren Fall abdecken, sie sollte jedoch plausibel einen Weg aufzeigen, der interessierte Personen durch die Rechtsnormen leitet.

Als Alternative regt der HmbBfDI an, dass die Formulierung zumindest die wichtigsten Rechtsgrundlagen benennt, bspw.:

„Wir verarbeiten diese Daten nur im Rahmen der von Ihnen genutzten Dienste und verwenden sie nur auf der Grundlage von Art. 6 Abs. 1 e) DSGVO, in Verbindung mit § 8 Online-Zugangsgesetz (OZG), § 4 Hamburgisches Datenschutzgesetz (HmbDSG), § 25 Telekommunikation-Telemedienschutz-Gesetz (TTDSG). Je nach Anwendung sind weitere Fachgesetze wie beispielsweise das Meldegesetz relevant. Hierzu finden Sie ggf. gesonderte Informationen bei den jeweiligen Services.“

Mit freundlichen Grüßen,

Felix Wagner

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de

Website: datenschutz-hamburg.de

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Von: [REDACTED]
An: [Wagner, Felix](#)
Cc: [Wirth, Sebastian Dr.](#); [REDACTED]
Betreff: AW: Hamburg Serviceportal, Az. 3627/2021
Datum: Montag, 14. Februar 2022 08:17:58

Sehr geehrter Herr Wagner,
vielen Dank für den Hinweis und Ihren konstruktiven Vorschlag.

Wir besprechen das intern und melden uns zeitnah bei Ihnen dazu.

Herzlichen Gruß

[REDACTED]

Von: Wagner, Felix <felix.wagner@datenschutz.hamburg.de>
Gesendet: Freitag, 11. Februar 2022 17:44
An: [REDACTED]
Cc: Wirth, Sebastian Dr. <sebastian.wirth@datenschutz.hamburg.de>; [REDACTED]
[REDACTED]
Betreff: Hamburg Serviceportal, Az. 3627/2021

Sehr geehrte Frau [REDACTED],
sehr geehrte Damen und Herren,

Der HmbBfDI hat eine Beschwerde über das Hamburg ServicePortal erhalten (<https://serviceportal.hamburg.de/>). Die Beschwerde betrifft weitestgehend Einzelheiten, die der HmbBfDI nicht als datenschutzrechtlich problematisch beurteilt. Einer der Beschwerdegegenstände bezieht sich auf die Nennung der Rechtsgrundlage in der zugehörigen Datenschutzerklärung (<https://serviceportal.hamburg.de/HamburgGateway/FVP/FV/BasisHilfe/Datenschutz.aspx>). Dort heißt es:

„Wir verarbeiten diese Daten nur im Rahmen Ihres Auftrags und verwenden sie nur unter Beachtung der gesetzlichen Bestimmungen (Onlinezugangsgesetz (OZG), Hamburgisches Datenschutzgesetz, EU Datenschutzgrundverordnung (DSGVO), Telekommunikationsgesetz, Telemediengesetz sowie einschlägige Fachgesetze wie beispielsweise das Meldegesetz).“

Der HmbBfDI stimmt der Beschwerde insoweit zu, dass diese sehr pauschale Formulierung wohl nicht die Informationspflicht gem. Art. 13 Abs. 1 c) DSGVO erfüllt. Die Nennung der Rechtsgrundlage soll betroffene Personen in die Lage versetzen, eine belastbare Prüfung der zugrunde gelegten Rechtsnormen vorzunehmen (vgl. *Paal/Hennemann*, in: Paal/Paaly, DS-GVO BDSG, 3. Aufl. 2021, Art. 13 DSGVO, Rn. 16a).

Der HmbBfDI geht davon aus, dass der Ausgangspunkt der Verarbeitung stets Art. 6 Abs. 1 e) DSGVO sein dürfte, in Verbindung mit den jeweiligen Fachgesetzen. Aus Sicht des HmbBfDI muss die Benennung der Rechtsgrundlage zwar nicht jeden denkbaren Fall abdecken, sie sollte jedoch plausibel einen Weg aufzeigen, der interessierte Personen durch die Rechtsnormen leitet.

Als Alternative regt der HmbBfDI an, dass die Formulierung zumindest die wichtigsten Rechtsgrundlagen benennt, bspw.:

„Wir verarbeiten diese Daten nur im Rahmen der von Ihnen genutzten Dienste und verwenden sie nur auf der Grundlage von Art. 6 Abs. 1 e) DSGVO, in Verbindung mit § 8 Online-Zugangsgesetz (OZG), § 4 Hamburgisches Datenschutzgesetz (HmbDSG), § 25 Telekommunikation-Telemediendatenschutz-Gesetz (TTDSG). Je nach Anwendung sind weitere Fachgesetze wie beispielsweise das Meldegesetz relevant. Hierzu finden Sie ggf. gesonderte Informationen bei den jeweiligen Services.“

Mit freundlichen Grüßen,

Felix Wagner

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de

Website: datenschutz-hamburg.de

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Von: [REDACTED]
An: [Wirth, Sebastian Dr.](mailto:Sebastian.Wirth@datenschutz.hamburg.de)
Cc: [REDACTED]
Betreff: AW: Auftragsverarbeitung OSI
Datum: Mittwoch, 19. Januar 2022 12:46:30

Lieber Herr Wirth,
die Verarbeitung wird über den Betriebsvertrag geregelt, V15192-1. Anbei sende ich Ihnen hiervon die Anlage 3. Dort steht im Bereich Payment noch der Stand von bisherigen Payment Provider, dies wird absehbar aktualisiert. Die Vertragsnummer ergänzen wir entsprechend in dem Dokument zur Verarbeitungstätigkeit - einen neuen Stand des Dokumentes darüber hinaus gibt es nicht.

Herzliche Grüße, [REDACTED]

Von: Wirth, Sebastian Dr. <sebastian.wirth@datenschutz.hamburg.de>
Gesendet: Freitag, 14. Januar 2022 12:23
An: [REDACTED]
Betreff: Auftragsverarbeitung OSI

Az.: 30.09-26

Hallo [REDACTED]

in der Beschreibung der Verarbeitungstätigkeit (Bearbeitungsstand 03.08.2020) zu OSI ist Dataport als Auftragsverarbeiter nach Art. 28 DSGVO genannt. Eine Auftragsnummer ist dort nicht angegeben. Nach Art. 28 Abs. 3 DSGVO erfolgt die Verarbeitung durch einen Auftragsverarbeiter auf der Grundlage eines Vertrages oder eines anderen Rechtsinstruments. Bitte senden Sie mir diesen Vertrag inkl. der ggf. enthaltenden Anlagen zu. Sollte es mittlerweile einen neuen Stand der Beschreibung Verarbeitungstätigkeit geben, senden Sie mir diesen bitte ebenfalls zu.

Mit freundlichem Gruß

Dr. Sebastian Wirth

--

Dr. Sebastian Wirth

Referat T
Referatsleiter für den technischen Datenschutz, T

Freie und Hansestadt Hamburg
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg
Geschäftsstelle: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

Durchwahl Büro: +49 (0)40 428 54-4053
E-Mail sebastian.wirth@datenschutz.hamburg.de
Webauftritt datenschutz-hamburg.de

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Der ITSK ist auf Seiten des Auftragnehmers für die Planung und Koordination von datenschutzrechtlichen Kontrollen des Auftraggebers im Rahmen der Auftragsdatenverarbeitung verantwortlich. Das beinhaltet insbesondere die Abstimmung von Terminen sowie die Sicherstellung der Verfügbarkeit von erforderlichen Personen und Ressourcen (z.B. Räumen oder Dokumenten für die Einsichtnahme vor Ort). Prüfungen wie Audits, Zertifizierungen o.ä. die über eine datenschutzrechtliche Kontrolle hinausgehen, sind nicht Teil der hier vereinbarten Leistung (vgl. Kapitel 2.7).

2.3 Grundschutzkonformer Betrieb

Der Auftragnehmer verpflichtet sich, die vom BSI in den IT-Grundschutzkatalogen⁴ vorgegebenen BASIS- und STANDARD-Anforderungen, die in den Zuständigkeitsbereich des Auftragnehmers fallen, für den von dieser Vereinbarung betroffenen Informationsverbund umzusetzen.

Die Identifikation und Umsetzung von Sicherheitsanforderungen erfolgt auf Basis der Bausteine der IT-Grundschutzkataloge in der beim Auftragnehmer eingesetzten Fassung und unter Einhaltung der für BSI-Zertifizierungen geltenden Übergangsfristen.

Die für den betrachteten Informationsverbund maßgeblichen Sicherheitsanforderungen und dessen jeweiliger Umsetzungsstand werden im Sicherheitskonzept dokumentiert. Sofern zusätzliche Sicherheitsanforderungen umgesetzt werden müssen, sind diese im SSLA Teil B zu benennen und dessen Umsetzung zu beauftragen.

2.4 Erstellung und Pflege der Sicherheitsdokumentation

2.4.1 Umfang

Der Auftragnehmer erstellt und pflegt ein in Form und Struktur standardisiertes, grundschutzkonformes Sicherheitskonzept und weist dem Auftraggeber auf dieser Basis den grundschutzkonformen Betrieb nach (Sicherheitsnachweis).

Das Sicherheitskonzept beschreibt die nach IT-Grundschutz-Methodik zusammengefasste Struktur des betrachteten Informationsverbundes sowie die maßgeblichen⁵ Sicherheitsanforderungen im Zuständigkeitsbereich des Auftragnehmers.

Der Auftragnehmer stellt die dauerhafte Umsetzung der Sicherheitsanforderungen sicher. Zu diesem Zweck prüft regelmäßig den Umsetzungsstand der Sicherheitsanforderungen und dokumentiert diesen im Sicherheitsnachweis.

Die Betrachtung und Prüfung von Sachverhalten im Verantwortungsbereich des Auftraggebers, die über die Leistungen nach Kapitel 2.5 hinausgehen, sind nicht Gegenstand der Leistungsvereinbarung.

2.4.2 Struktur und Standardordner

⁴ Die aktuelle Version der IT-Grundschutz-Kataloge kann beim BSI abgerufen werden (www.bsi.bund.de).

⁵ Die Festlegung der relevanten Sicherheitsanforderungen erfolgt auf Grundlage der Modellierungsvorschriften des BSI-Standards 200-2.

Von: [Wagner, Felix](#)
An: [REDACTED]
Betreff: AW: Hamburg Serviceportal, Az. 3627/2021
Datum: Montag, 14. März 2022 14:06:00

Sehr geehrte [REDACTED]

hat sich in dieser Sache zwischenzeitlich etwas ergeben?

Mit freundlichen Grüßen,

Felix Wagner

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de

Website: [datenschutz-hamburg.de](https://www.datenschutz-hamburg.de)

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Von: [REDACTED]

Gesendet: Montag, 14. Februar 2022 08:18

An: Wagner, Felix <felix.wagner@datenschutz.hamburg.de>

Cc: Wirth, Sebastian Dr. <sebastian.wirth@datenschutz.hamburg.de>; [REDACTED]
[REDACTED]
[REDACTED]

Betreff: AW: Hamburg Serviceportal, Az. 3627/2021

Sehr geehrter Herr Wagner,
vielen Dank für den Hinweis und Ihren konstruktiven Vorschlag.

Wir besprechen das intern und melden uns zeitnah bei Ihnen dazu.

Herzlichen Gruß

[REDACTED]

Von: Wagner, Felix <felix.wagner@datenschutz.hamburg.de>

Gesendet: Freitag, 11. Februar 2022 17:44

An: [REDACTED]

Cc: Wirth, Sebastian Dr. <sebastian.wirth@datenschutz.hamburg.de>; [REDACTED]

Betreff: Hamburg Serviceportal, Az. 3627/2021

Sehr geehrte [REDACTED]
sehr geehrte Damen und Herren,

Der HmbBfDI hat eine Beschwerde über das Hamburg ServicePortal erhalten (<https://serviceportal.hamburg.de/>). Die Beschwerde betrifft weitestgehend Einzelheiten, die der HmbBfDI nicht als datenschutzrechtlich problematisch beurteilt. Einer der Beschwerdegegenstände bezieht sich auf die Nennung der Rechtsgrundlage in der zugehörigen Datenschutzerklärung (<https://serviceportal.hamburg.de/HamburgGateway/FVP/FV/BasisHilfe/Datenschutz.aspx>). Dort heißt es:

„Wir verarbeiten diese Daten nur im Rahmen Ihres Auftrags und verwenden sie nur unter Beachtung der gesetzlichen Bestimmungen (Onlinezugangsgesetz (OZG), Hamburgisches Datenschutzgesetz, EU Datenschutzgrundverordnung (DSGVO), Telekommunikationsgesetz, Telemediengesetz sowie einschlägige Fachgesetze wie beispielsweise das Meldegesetz).“

Der HmbBfDI stimmt der Beschwerde insoweit zu, dass diese sehr pauschale Formulierung wohl nicht die Informationspflicht gem. Art. 13 Abs. 1 c) DSGVO erfüllt. Die Nennung der Rechtsgrundlage soll betroffene Personen in die Lage versetzen, eine belastbare Prüfung der zugrunde gelegten Rechtsnormen vorzunehmen (vgl. *Paal/Hennemann*, in: Paal/Paaly, DS-GVO BDSG, 3. Aufl. 2021, Art. 13 DSGVO, Rn. 16a).

Der HmbBfDI geht davon aus, dass der Ausgangspunkt der Verarbeitung stets Art. 6 Abs. 1 e) DSGVO sein dürfte, in Verbindung mit den jeweiligen Fachgesetzen. Aus Sicht des HmbBfDI muss die Benennung der Rechtsgrundlage zwar nicht jeden denkbaren Fall abdecken, sie sollte jedoch plausibel einen Weg aufzeigen, der interessierte Personen durch die Rechtsnormen leitet.

Als Alternative regt der HmbBfDI an, dass die Formulierung zumindest die wichtigsten Rechtsgrundlagen benennt, bspw.:

„Wir verarbeiten diese Daten nur im Rahmen der von Ihnen genutzten Dienste und verwenden sie nur auf der Grundlage von Art. 6 Abs. 1 e) DSGVO, in Verbindung mit § 8 Online-Zugangsgesetz (OZG), § 4 Hamburgisches Datenschutzgesetz (HmbDSG), § 25 Telekommunikation-Telemedienschutz-Gesetz (TTDSG). Je nach Anwendung sind weitere Fachgesetze wie beispielsweise das Meldegesetz relevant. Hierzu finden Sie ggf. gesonderte Informationen bei den jeweiligen Services.“

Mit freundlichen Grüßen,

Felix Wagner

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de

Website: datenschutz-hamburg.de

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Von: [Wagner, Felix](#)
An: [REDACTED]
Betreff: WG: Hamburg Serviceportal, Az. 3627/2021
Datum: Mittwoch, 30. März 2022 14:50:00

Sehr geehrte [REDACTED],

unsererseits ist leider immer noch nicht klar, ob sich in dieser Sache nun etwas Weiteres ergeben wird. Hat die interne Besprechung dazu stattgefunden?

Mit freundlichen Grüßen,

Felix Wagner

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de

Website: [datenschutz-hamburg.de](https://www.datenschutz-hamburg.de)

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Von: Wagner, Felix

Gesendet: Montag, 14. März 2022 14:06

An: [REDACTED]

Betreff: AW: Hamburg Serviceportal, Az. 3627/2021

Sehr geehrte [REDACTED]

hat sich in dieser Sache zwischenzeitlich etwas ergeben?

Mit freundlichen Grüßen,

Felix Wagner

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de

Website: [datenschutz-hamburg.de](https://www.datenschutz-hamburg.de)

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Von: [REDACTED]

Gesendet: Montag, 14. Februar 2022 08:18

An: Wagner, Felix <felix.wagner@datenschutz.hamburg.de>

Cc: Wirth, Sebastian Dr. <sebastian.wirth@datenschutz.hamburg.de>; [REDACTED]
[REDACTED]
[REDACTED]

Betreff: AW: Hamburg Serviceportal, Az. 3627/2021

Sehr geehrter Herr Wagner,
vielen Dank für den Hinweis und Ihren konstruktiven Vorschlag.

Wir besprechen das intern und melden uns zeitnah bei Ihnen dazu.

Herzlichen Gruß

[REDACTED]

Von: Wagner, Felix <felix.wagner@datenschutz.hamburg.de>

Gesendet: Freitag, 11. Februar 2022 17:44

An: [REDACTED]

Cc: Wirth, Sebastian Dr. <sebastian.wirth@datenschutz.hamburg.de>; [REDACTED]
[REDACTED]

Betreff: Hamburg Serviceportal, Az. 3627/2021

Sehr geehrte [REDACTED]
sehr geehrte Damen und Herren,

Der HmbBfDI hat eine Beschwerde über das Hamburg ServicePortal erhalten (<https://serviceportal.hamburg.de/>). Die Beschwerde betrifft weitestgehend Einzelheiten, die der HmbBfDI nicht als datenschutzrechtlich problematisch beurteilt. Einer der Beschwerdegegenstände bezieht sich auf die Nennung der Rechtsgrundlage in der zugehörigen Datenschutzerklärung (<https://serviceportal.hamburg.de/HamburgGateway/FVP/FV/BasisHilfe/Datenschutz.aspx>). Dort heißt es:

„Wir verarbeiten diese Daten nur im Rahmen Ihres Auftrags und verwenden sie nur unter Beachtung der gesetzlichen Bestimmungen (Onlinezugangsgesetz (OZG), Hamburgisches Datenschutzgesetz, EU Datenschutzgrundverordnung (DSGVO), Telekommunikationsgesetz, Telemediengesetz sowie einschlägige Fachgesetze wie beispielsweise das Meldegesetz).“

Der HmbBfDI stimmt der Beschwerde insoweit zu, dass diese sehr pauschale Formulierung wohl nicht die Informationspflicht gem. Art. 13 Abs. 1 c) DSGVO erfüllt. Die Nennung der

Rechtsgrundlage soll betroffene Personen in die Lage versetzen, eine belastbare Prüfung der zugrunde gelegten Rechtsnormen vorzunehmen (vgl. *Paal/Hennemann*, in: Paal/Paaly, DS-GVO BDSG, 3. Aufl. 2021, Art. 13 DSGVO, Rn. 16a).

Der HmbBfDI geht davon aus, dass der Ausgangspunkt der Verarbeitung stets Art. 6 Abs. 1 e) DSGVO sein dürfte, in Verbindung mit den jeweiligen Fachgesetzen. Aus Sicht des HmbBfDI muss die Benennung der Rechtsgrundlage zwar nicht jeden denkbaren Fall abdecken, sie sollte jedoch plausibel einen Weg aufzeigen, der interessierte Personen durch die Rechtsnormen leitet.

Als Alternative regt der HmbBfDI an, dass die Formulierung zumindest die wichtigsten Rechtsgrundlagen benennt, bspw.:

„Wir verarbeiten diese Daten nur im Rahmen der von Ihnen genutzten Dienste und verwenden sie nur auf der Grundlage von Art. 6 Abs. 1 e) DSGVO, in Verbindung mit § 8 Online-Zugangsgesetz (OZG), § 4 Hamburgisches Datenschutzgesetz (HmbDSG), § 25 Telekommunikation-Telemediendatenschutz-Gesetz (TTDSG). Je nach Anwendung sind weitere Fachgesetze wie beispielsweise das Meldegesetz relevant. Hierzu finden Sie ggf. gesonderte Informationen bei den jeweiligen Services.“

Mit freundlichen Grüßen,

Felix Wagner

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de

Website: [datenschutz-hamburg.de](https://www.datenschutz-hamburg.de)

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Von: [REDACTED]
An: [Wagner, Felix](#)
Betreff: AW: Hamburg Serviceportal, Az. 3627/2021
Datum: Donnerstag, 31. März 2022 15:30:11

Sehr geehrter Herr Wagner,
vielen Dank für Ihre Nachfrage (ich war ein bisschen mit Corona beschäftigt).

Inhaltlich haben Sie völlig Recht. Wir werden die Änderung so schnell wie möglich einfügen (lassen).

Ich sage Ihnen Bescheid, zu wann das geplant ist (es bedarf da meist ein wenig Vorlauf).

Herzlichen Gruß

[REDACTED]

Von: Wagner, Felix <felix.wagner@datenschutz.hamburg.de>
Gesendet: Mittwoch, 30. März 2022 14:51
An: [REDACTED]
Betreff: WG: Hamburg Serviceportal, Az. 3627/2021

Sehr geehrte [REDACTED]

unsererseits ist leider immer noch nicht klar, ob sich in dieser Sache nun etwas Weiteres ergeben wird. Hat die interne Besprechung dazu stattgefunden?

Mit freundlichen Grüßen,

Felix Wagner

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg
Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg
Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de
Website: [datenschutz-hamburg.de](https://www.datenschutz-hamburg.de)

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Von: Wagner, Felix
Gesendet: Montag, 14. März 2022 14:06
An: [REDACTED]
Betreff: AW: Hamburg Serviceportal, Az. 3627/2021

Sehr geehrte [REDACTED]

hat sich in dieser Sache zwischenzeitlich etwas ergeben?

Mit freundlichen Grüßen,

Felix Wagner

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de

Website: datenschutz-hamburg.de

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Von: [REDACTED]

Gesendet: Montag, 14. Februar 2022 08:18

An: Wagner, Felix <felix.wagner@datenschutz.hamburg.de>

Cc: Wirth, Sebastian Dr. <sebastian.wirth@datenschutz.hamburg.de>; [REDACTED]
[REDACTED]
[REDACTED]

Betreff: AW: Hamburg Serviceportal, Az. 3627/2021

Sehr geehrter Herr Wagner,
vielen Dank für den Hinweis und Ihren konstruktiven Vorschlag.

Wir besprechen das intern und melden uns zeitnah bei Ihnen dazu.

Herzlichen Gruß

[REDACTED]

Von: Wagner, Felix <felix.wagner@datenschutz.hamburg.de>

Gesendet: Freitag, 11. Februar 2022 17:44

An: [REDACTED]

Cc: Wirth, Sebastian Dr. <sebastian.wirth@datenschutz.hamburg.de>; [REDACTED]
[REDACTED]

Betreff: Hamburg Serviceportal, Az. 3627/2021

Sehr geehrte [REDACTED]

sehr geehrte Damen und Herren,

Der HmbBfDI hat eine Beschwerde über das Hamburg ServicePortal erhalten (<https://serviceportal.hamburg.de/>). Die Beschwerde betrifft weitestgehend Einzelheiten, die der HmbBfDI nicht als datenschutzrechtlich problematisch beurteilt. Einer der Beschwerdegegenstände bezieht sich auf die Nennung der Rechtsgrundlage in der zugehörigen Datenschutzerklärung (<https://serviceportal.hamburg.de/HamburgGateway/FVP/FV/BasisHilfe/Datenschutz.aspx>). Dort heißt es:

„Wir verarbeiten diese Daten nur im Rahmen Ihres Auftrags und verwenden sie nur unter Beachtung der gesetzlichen Bestimmungen (Onlinezugangsgesetz (OZG), Hamburgisches Datenschutzgesetz, EU Datenschutzgrundverordnung (DSGVO), Telekommunikationsgesetz, Telemediengesetz sowie einschlägige Fachgesetze wie beispielsweise das Meldegesetz).“

Der HmbBfDI stimmt der Beschwerde insoweit zu, dass diese sehr pauschale Formulierung wohl nicht die Informationspflicht gem. Art. 13 Abs. 1 c) DSGVO erfüllt. Die Nennung der Rechtsgrundlage soll betroffene Personen in die Lage versetzen, eine belastbare Prüfung der zugrunde gelegten Rechtsnormen vorzunehmen (vgl. *Paal/Hennemann*, in: Paal/Paaly, DS-GVO BDSG, 3. Aufl. 2021, Art. 13 DSGVO, Rn. 16a).

Der HmbBfDI geht davon aus, dass der Ausgangspunkt der Verarbeitung stets Art. 6 Abs. 1 e) DSGVO sein dürfte, in Verbindung mit den jeweiligen Fachgesetzen. Aus Sicht des HmbBfDI muss die Benennung der Rechtsgrundlage zwar nicht jeden denkbaren Fall abdecken, sie sollte jedoch plausibel einen Weg aufzeigen, der interessierte Personen durch die Rechtsnormen leitet.

Als Alternative regt der HmbBfDI an, dass die Formulierung zumindest die wichtigsten Rechtsgrundlagen benennt, bspw.:

„Wir verarbeiten diese Daten nur im Rahmen der von Ihnen genutzten Dienste und verwenden sie nur auf der Grundlage von Art. 6 Abs. 1 e) DSGVO, in Verbindung mit § 8 Online-Zugangsgesetz (OZG), § 4 Hamburgisches Datenschutzgesetz (HmbDSG), § 25 Telekommunikation-Telemediendatenschutz-Gesetz (TTDSG). Je nach Anwendung sind weitere Fachgesetze wie beispielsweise das Meldegesetz relevant. Hierzu finden Sie ggf. gesonderte Informationen bei den jeweiligen Services.“

Mit freundlichen Grüßen,

Felix Wagner

Referent für Datenschutz

Referat M

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsst.: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

E-Mail: felix.wagner@datenschutz.hamburg.de

Website: datenschutz-hamburg.de

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.

Von: [Wirth, Sebastian Dr.](#)
An: ["c.franke.6.zhuffu83u@fragdenstaat.de"](mailto:c.franke.6.zhuffu83u@fragdenstaat.de)
Betreff: Sicherheit des Verwaltungsportals
Datum: Dienstag, 7. Juni 2022 13:33:00
Anlagen: [20220607 Stellungnahme HmbBfDI_T.pdf](#)

Az.: 3627_2021

Guten Tag Frau Franke,

in der Anlage übersende ich Ihnen die Stellungnahme des HmbBfDI zu Ihrer Anfrage.

Mit freundlichem Gruß

Dr. Sebastian Wirth

--

Dr. Sebastian Wirth

Referat T

Referatsleiter für den technischen Datenschutz, T

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsstelle: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

Durchwahl Büro: +49 (0)40 428 54-4053

E-Mail sebastian.wirth@datenschutz.hamburg.de

Webauftritt datenschutz-hamburg.de

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns übermittelt werden sollten.



Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Ludwig-Erhard-Str. 22, 20459 Hamburg

Frau Franke

Ludwig-Erhard-Str. 22, 7. OG
20459 Hamburg
Telefon: 040 - 428 54 - 40 53 Zentrale - 40 40
Telefax: 040 - 428 54 - 40 00
Ansprechpartner: Herr Dr. Sebastian Wirth
Referat T (Technik)
E-Mail*: Sebastian.Wirth@datenschutz.hamburg.de

Az.: T / 3627_2021

Hamburg, den 07.06.2022.

nur per Mail

Sicherheit des Hamburgischen Verwaltungsportals

Guten Tag Frau Franke,

vielen Dank für Ihre Nachricht vom 19.11.2021 in der Sie Bedenken äußern, dass bei Nutzerkonten im hamburgischen Serviceportal die erforderlichen Maßnahmen nach Art 23 DSGVO nicht erfüllt werden. Hierzu möchte ich zu den Aspekten Stellung nehmen, die Sie in Bezug auf das Servicekonto Hamburg in Ihrer Eingabe aufgeführt haben.

Abweichung der Domänen zwischen Portal und Mail-Domäne

Die Registrierung eines Nutzerkontos in OSI erfolgt unter <https://servicekonto.serviceportal.hamburg.de/servicekonto/>. Nach der ersten Registrierung erhalten die Nutzer:innen im Nutzerkonto zur Aktivierung des Nutzerkontos in OSI einen Link per Mail mit der Absender-Adresse noreply_serviceportal-hamburg@dataport.de.

Die Domäne des Nutzerkontos und des Absenders der Mail mit dem verschickten Aktivierungs-Links unterscheiden sich. In der Datenschutzerklärung und in den Hilfetexten von A-Z des Serviceportals wird jedoch die Mailadresse meinServiceportal@dataport.de explizit als Kontaktadresse für Fragen zur Registrierung zum Nutzerkonto genannt. Diese Mailadresse für Fragen zur Registrierung kommt aus derselben Domäne wie die Mail, mit der das Nutzerkonto aktiviert werden muss. Die Nutzer:innen können somit leicht die Herkunft der Mail beim Registrierungsprozess nachvollziehen.

Verpflichtung zum Postfach

Die Rechtsgrundlage der Verarbeitung der Daten in den Nutzerkonten und den Postfächern ist das Online-Zugangsgesetz, insbesondere in den §2 Abs. 7, §8 Abs. 4 und §9 Abs. 1. OZG. Diese gesetzlichen Grundlagen der Datenverarbeitung inkorporieren die Einwilligungen bzw. Zustimmungen als bloßes Tatbestandsmerkmale. Die Rechtsgrundlage der Verarbeitung ist somit nicht die Einwilligung gemäß Art. 6 Abs. 1a DSGVO.

Website:
www.datenschutz-hamburg.de

E-Mail Sammelpostfach*:
mailbox@datenschutz.hamburg.de

Öffentliche Verkehrsmittel:
S-Bahnen S1, S2, S3 (Station Stadthausbrücke),
U-Bahn U3 (Station St. Pauli), Busse 6 und 37

*Vertrauliche Informationen sollten auf elektronischem Weg nur verschlüsselt an uns übermittelt werden.
Unser öffentlicher PGP-Schlüssel ist im Internet verfügbar (Fingerprint: 0932 579B 33C1 8C21 6C9D E77D 08DD BAE4 3377 5707)

Das OZG wurde bezüglich der Postfächer im Dezember 2020 geändert. In der Bundestagsdrucksache Drucksache 19/23774 vom 28.10.2020 ist in der Begründung zu dieser Änderung unter Ziffer Zu Nummer 1 Buchstabe d ausgeführt:

"Eine vollständige Kommunikation zwischen Nutzern und der Verwaltung umfasst nicht nur die Beantragung einer Verwaltungsleistung, sondern auch den sog. Rückkanal, insbesondere also die digitale Übermittlung der Entscheidung der Behörde an den Nutzer (bidirektionale Kommunikation). Hierzu stellen Bund und Länder im Rahmen des Aufbaus der Nutzerkonten sog. Postfächer bereit. Postfächer sind ein wesentlicher Basisdienst, um Mitteilungen, Bescheide und Benachrichtigungen zum Bearbeitungsstatus medienbruchfrei und nutzerfreundlich elektronisch bereitzustellen, die anschließend vom Nutzer abgerufen werden können. Die Kenntnisnahme bzw. das Herunterladen dieser Informationen durch den Nutzer setzt eine dem Vertrauensniveau der Verwaltungsleistung angemessene Authentisierung voraus. Das Postfach wurde bisher lediglich in der amtlichen Begründung zum OZG erwähnt und wird daher mit dieser Änderung in die Begriffsbestimmungen des OZG aufgenommen. Die Gestaltung des Postfachs ist technikoffen. Die Möglichkeit, mehrere Postfächer, insbesondere im Rahmen von Organisationskonten zu nutzen, ist nicht ausgeschlossen."

Nutzerkonten dienen der bidirektionalen Kommunikation zwischen Nutzer:innen und Behörde. Dies setzt voraus, dass mit der Registrierung und Anlage eines Nutzerkontos auch ein Postfach als Komponente des Nutzerkontos bereitgestellt wird. Mit dieser Komponente wird eine Möglichkeit geschaffen den Betroffenen medienbruchfrei bezüglich einer Anfrage oder eines Antrags zu antworten.

Datenschutzerklärung

Der HmbBfDI hat Ihre Anfrage zum Anlass genommen, sich mit der Senatskanzlei Hamburg als verantwortliche Stelle darüber zu verständigen, zukünftig in der Datenschutzerklärung eine differenzierte Darstellung der Rechtsgrundlage der Verarbeitung der personenbezogenen Daten mit aufzunehmen. Die Senatskanzlei hat angekündigt, diese Veränderung kurzfristig umzusetzen.

Auftragsdatenverarbeitung

Für den Betrieb der Online Service Infrastruktur wurde ein Auftragsverarbeitungsvertrag geschlossen. In diesem Vertrag wurde ein grundschutzkonformer Betrieb auf der Basis der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgegebenen BASIS- und STAN-DARD-Anforderungen festgeschrieben. Eine ständige Fortschreibung der erforderlichen Maßnahmen ist ebenfalls Gegenstand des Vertrags. Um einem erhöhten Schutzbedarf der verarbeiteten Daten Rechnung zu tragen, wurden zusätzliche Schutzmaßnahmen vereinbart. Dazu gehören u.a. Maßnahmen zur Verschlüsselung bei der Datenübertragung. Auch die Durchführung regelmäßiger Penetrationstests ist vorgesehen.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichem Gruß

Dr. Sebastian Wirth

Von: [Christina Franke \[#233299\]](#)
An: [Wirth, Sebastian Dr.](#)
Betreff: [EXTERN]-AW: Sicherheit des Verwaltungsportals [#233299]
Datum: Freitag, 17. Juni 2022 13:25:37

Sehr geehrte Herr Dr. Wirth,

angesichts der Veröffentlichung von Herrn Lindenberg auf <https://blog.lindenberg.one/BeschwerdeDataport> - die dem Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ja bekannt sind, einschließlich der mangelhaften Sicherheitskonzepte - empfinde ich Ihr Schreiben als allzu dünn und ausweichend. Insbesondere Ihre Ausführungen zu den Maßnahmen sind mindestens so dünn wie die Verträge selbst. Auch weichen Sie der Feststellung dass nicht oder nicht konsequent verschlüsselt gespeichert wird und damit Schutzbedarf hoch - wie festgestellt - nicht erreicht wird gekonnt aus, indem Sie nur auf verschlüsselte Übertragung eingehen.

Warum traut sich die Aufsicht nicht, ein Sicherheitskonzept entsprechend dem Stand der Technik und den Risiken - die ja selbst das BSI als gegeben ansieht - einzufordern?

Mit freundlichen Grüßen
Christina Franke

Anfragen: 233299
Antwort an: c.franke.6.zhufhf83u@fragdenstaat.de

Laden Sie große Dateien zu dieser Anfrage hier hoch:
<https://fragdenstaat.de/anfrage/233299/upload/06e680fa5f16aed3d7697fea7383b5a84e1dfdaa/>

--

Rechtshinweis: Diese E-Mail wurde über den Webservice fragdenstaat.de versendet. Antworten werden ggf. im Auftrag der Antragstellenden auf dem Internet-Portal veröffentlicht.

Falls Sie Fragen dazu haben oder eine Idee, was für eine Anfrage bei Ihnen im Haus notwendig wäre, besuchen Sie:

<https://fragdenstaat.de/fuer-behoerden/>

Von: Wirth, Sebastian Dr.
An: ["c.franke.6.zhuffu83u@fragdenstaat.de"](mailto:c.franke.6.zhuffu83u@fragdenstaat.de)
Betreff: Sicherheit des Verwaltungsportals
Datum: Donnerstag, 25. August 2022 15:57:00

Az.: 3627_2021

Guten Tag Frau Franke,

vielen Dank für Ihre Nachfrage vom 17.06.2022. Dazu möchte ich gerne erläutern, dass sich der HmbBfDI in seinen Kontakten zu Verantwortlichen einer Verarbeitungstätigkeit nachdrücklich dafür einsetzt, den Stand der Technik durch entsprechende technische und organisatorische Maßnahmen zu erreichen. Der IT-Grundschutz liefert hierfür ein fachliches Fundament und ein umfangreiches Arbeitswerkzeug. Er ist Methode, Anleitung, Empfehlung und Hilfe zur Selbsthilfe für Behörden, Unternehmen und Institutionen, die sich mit der Absicherung ihrer Daten, Systeme und Informationen befassen. Die IT-Grundschutzbausteine geben dazu wichtige konkrete Empfehlungen. Im Zuge seiner Aufgabenwahrnehmung bezieht der HmbBfDI dabei auch spezifische und allgemeine Hinweise von Bürgerinnen und Bürgern zu konkreten Verarbeitungstätigkeiten ein.

Den rechtliche Rahmen für die zu treffenden Schutzmaßnahmen bildet insbesondere Art. 32 DSGVO, in dem festgeschrieben ist, dass die Verantwortlichen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Den Verantwortlichen stehen dabei in der Regelfall verschiedene sich ergänzende aber auch alternativ nutzbare Maßnahmen zur Verfügung. Eine Bewertung ist vor diesem Hintergrund immer nur spezifisch möglich.

Mit freundlichem Gruß

Dr. Sebastian Wirth

--

Dr. Sebastian Wirth

Referat T

Referatsleiter für den technischen Datenschutz, T

Freie und Hansestadt Hamburg

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit

Anschrift: Ludwig-Erhard-Str. 22 · 20459 Hamburg

Geschäftsstelle: Telefon: +49 (0)40 428 54-4040 Fax: +49 (0)40 428 54-4000

Durchwahl Büro: +49 (0)40 428 54-4053

E-Mail sebastian.wirth@datenschutz.hamburg.de

Webauftritt datenschutz-hamburg.de

Abhängig vom Anlass Ihrer oder unserer Kontaktaufnahme werden Ihre personenbezogenen Daten von uns verarbeitet. Nähere Informationen dazu erhalten Sie [hier](#) oder auf Nachfrage bei unserer behördlichen Datenschutzbeauftragten.

Bitte beachten Sie auch, dass vertrauliche Informationen auf elektronischem Wege nur verschlüsselt an uns

übermittelt werden sollten.