Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

LDI NRW, Postfach 20 04 44, 40102 Düsseldorf

Joachim Lindenberg
Heubergstr. 1a
76228 Karlsruhe

Aktenzeichen
bei Antwort bitte angeben
23.T5.1.2-5615/23
Referat-23@ldi.nrw.de

[redacted]
Telefon 0211 38424-[redacted]
Fax 0211 38424-999

Ihre E-Mail vom 22.03.2024

Sehr geehrter Herr Lindenberg,

vielen Dank für Ihre E-Mail vom 22. März 2024.

Im Anhang übersende ich Ihnen erneut die angeforderte Stellungnahme der verantwortlichen Stelle zu Ihrer Eingabe mit dem Aktenzeichen 23.T5.1.2-5615/23.

Die verantwortliche Stelle hatte zum Zeitpunkt Ihrer Beschwerde vom 04.08.2023 nach eigener Auskunft lediglich eine opportunistische Transportverschlüsselung implementiert. Sofern die empfangende Stelle keine Transportverschlüsselung unterstützt oder ein gezielter Angriff auf dieses Verfahren erfolgt, hätte es in Einzelfällen zu einer unverschlüsselten Übertragung kommen können. Da allerdings mittlerweile von allen gängigen Providern eine Transportverschlüsselung implementiert wird, ist die Eintrittswahrscheinlichkeit dieser Einzelfälle als gering einzustufen. Darüber hinaus möchte ich darauf hinweisen, dass es sich bei der von Ihnen durchgeführten Downgrade-Attacke um eine von Ihnen selbst bewusste Herbeiführung einer unverschlüsselten Übermittlung Ihrer personenbezogenen Daten gehandelt hat. Weitere Vorfälle dieser Art sind mir in Bezug auf die verantwortliche Stelle nicht bekannt.

Nach meinem Hinweis hat die verantwortliche Stelle umgehend eine obligatorische Transportverschlüsselung eingeführt, sodass das verbleibende Restrisiko möglicher Einzelfälle einer unverschlüsselten Übertragung nunmehr hinreichend adressiert ist.

Dienstgebäude und
Lieferanschrift:
Kavalleriestraße 2 - 4
40213 Düsseldorf
Telefon 0211 38424-0
Telefax 0211 38424-999
poststelle@ldi.nrw.de
www.ldi.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 704, 709, 719
Haltestelle Poststraße

Hinsichtlich des von Ihnen vermuteten weiteren Verstoßes aufgrund einer Nichtzustellung von E-Mails bei der Durchführung einer Downgrade-Attacke und der damit unterbundenen unverschlüsselten Übertragung verweise ich auf mein Schreiben vom 19.03.2024, in welchem dieser Punkt bereits adressiert wurde.

Mir liegen ferner keine Hinweise vor, dass die in der Stellungnahme der verantwortlichen Stelle ausgeführte technische Umsetzung für die Passwortwiederherstellung nicht datenschutzkonform ausgestaltet ist. Ein Aufgreifen dieses Punkts im Rahmen meiner aufsichtsrechtlichen Tätigkeit ist daher nicht angezeigt.

Weiter erlaube ich mir, Sie darauf hinzuweisen, dass die LDI NRW als Datenschutz-Aufsichtsbehörde, wie bereits mehrfach gerichtlich festgestellt, unabhängig ist und ihr aufsichtsbehördliches Einschreiten nach pflichtgemäßem Ermessen – orientiert an dem Grundsatz der Verhältnismäßigkeit – entscheidet (Art. 77 a Verfassung für das Land Nordrhein-Westfalen, § 25 Abs. 2 DSG NRW). So hat eine Beschwerdeführerin oder ein Beschwerdeführer lediglich einen Anspruch darauf, dass ihre/seine Eingabe entgegengenommen, ermessensgerecht geprüft sowie die Datenschutz-Grundverordnung bei Bedarf ermessensgerecht durchgesetzt wird, nicht aber einen Anspruch darauf, dass das von ihr/ihm angestrebte Ergebnis auch tatsächlich herauskommt.

Rechtsbehelfsbelehrung

Gegen diesen Bescheid können Sie innerhalb eines Monats Klage beim Verwaltungsgericht Düsseldorf erheben.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

einfach-einreichen – Ein Service der AfP GmbH · Feldstiege 72 · 48161 Münster

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen
[redacted]
Kavalleriestraße 2-4
40213 Düsseldorf

Münster, 25.10.2023

Anforderung von Auskünften nach Art. 58 Abs 1 lit. a DSGVO - Aktenzeichen T5.1.2-5615/23

Sehr geehrter [redacted],

bezugnehmend zu Ihrem Schreiben vom 28.09.2023 kommen wir hiermit Ihrer Anforderung der Auskunft nach Art. 58 Abs. 1 lit. a DSGVO nach.

1. Im Fall einer Registrierung beim Portal www.einfach-einreichen.de wird eine E-Mail zwecks Validierung der angegebenen E-Mailadresse mit folgenden Kategorien verschickt:
   a. Vorname Name
   b. E-Mail-Adresse

   Nach erfolgreicher Erstanmeldung sind im Portal, neben den bei der Registrierung angegebenen Daten keine weiteren Daten ersichtlich. Infolge der vorgesehenen Nutzung des Portals verwaltet der Nutzer, durch sein eigenes Handeln (hochladen von Dateien/Dokumenten) oder durch den Empfang von elektronischen Rechnungen Gesundheitsdaten.

2. Das Risiko für die Rechte und Freiheiten natürlicher Personen, welches mit dem Versand von E-Mails durch das Portal einhergeht, ist als gering zu betrachten. Zum einen, durch die starke Begrenzung der Daten auf ein minimales Maß, die in den durch das Portal versendeten E-Mails enthalten sind (siehe oben) und zum anderen erfolgt die Anmeldung an das Portal www.einfach-einreichen.de mittels zweistufiger Authentifizierung (2FA), welches der Nutzer verpflichtend aktivieren muss, um Dokumente empfangen/verwalten zu können.

3. Die Konfiguration des Mailservers wurde zwischenzeitlich unter Einbezug der Orientierungshilfe "Maßnahmen zum Schutz personenbezogener Daten bei Übermittlung per E-Mail" (Kapitel 4.2.1 resp. 5.1.), auf das Erfordernis einer obligatorischen Transportverschlüsselung (TLS erforderlich) angepasst.

4. Für das Zurücksetzen des Passworts für das Portal www.einfach-einreichen.de erzeugt der Nutzer durch Auswahl der Option "Passwort vergessen" und Eingabe seiner für den Zugang verwendeten E-Mail-Adresse eine E-Mail, welche an die angegebene E-Mail-Adresse versendet wird. Mittels eines zeitlich begrenzten, persönlichen Links in der E-Mail gelangt der Nutzer auf eine Seite im Portal auf der er seinen Wiederherstellungscode eingeben muss. Nach erfolgter Eingabe des Wiederherstellungscodes kann der Nutzer sein Passwort zurücksetzen. Für den Wiederherstellungscode stehen dem Nutzer zwei

Varianten zur Verfügung. Der Nutzer wählt seine favorisierte Variante bei der Aktivierung des 2FA-Verfahrens aus. Hierbei kann der Nutzer zwischen einer Variante wählen, bei dem dieser den Wiederherstellungscode angezeigt bekommt und diesen notiert und eigenständig verwahrt oder einer Variante, bei dem der Nutzer seine Mobilfunknummer hinterlegt, an welche der Wiederherstellungscode im Bedarfsfall übermittelt wird. Im Vorfeld wird die Mobilfunknummer, analog der E-Mail-Adresse bei der Registrierung, mittels SMS inkl. Freischaltcode validiert/aktiviert. Abschließend noch zu erwähnen, dass es technisch ausgeschlossen ist (Privacy by Design), dass die AfP Zugriff auf den Wiederherstellungscode hat oder an diesen erlangen kann.
In dem Fall, dass der Nutzer in dem Portal keine Dokumente verwaltet bzw. infolgedessen kein 2FA aktiviert ist, erfolgt das Zurücksetzen des Zugangs ohne Wiederherstellungscode.

Gemäß unserer Abwägung – siehe Punkt 2 – haben wir keine weiteren Maßnahmen getroffen, als die Umsetzung der obligatorischen Transportverschlüsselung - siehe Punkt 3.

Wir hoffen ihr Auskunftsersuchen hinreichend erfüllt zu haben.

Mit freundlichen Grüßen

[redacted]

Datenschutzbeauftragter
AfP-Abrechnungsservice für Privatpatienten GmbH

einfach-einreichen –
Ein Service der AfP Abrechnungsservice für Privatpatienten GmbH
Feldstiege 72 · 48161 Münster

T 02533 6214900
E info@einfach-einreichen.de
W einfach-einreichen.de

Amtsgericht Charlottenburg
Sitz Berlin · HRB 202725
Steuer-Nr. 336/5777/2443

Geschäftsführer Alexander Dallmer, Jörg Matheis

Deutsche Apotheker- und Ärztebank
IBAN · DE17 3006 0601 0004 5592 40
BIC · DAAEDEDDXXX