PLANIT // LEGAL

// Kurzgutachten

zum Prüfungsbericht für den Datenschutznachweis nach § 18 Abs. 3 Nr. 4 des De-Mail-Gesetzes

Für die

FP Digital Business Solutions GmbH

Griesbergstr. 8

31162 Bad Salzdetfurth

Sachverständiger Prüfer (Recht und Technik)

Dr. Bernhard Freund, LL.M. (Wellington), M.Comp.Sc.

PLANIT // LEGAL Rechtsanwaltsgesellschaft mbH

Jungfernstieg 1

20095 Hamburg

Inhalt

A. Zeitpunkt und Ablauf der Prüfung

Wesentliche Grundlage der Prüfung war ein Vor-Ort-Audit am Standort der FP Digital Business Solutions GmbH in Fürstenwalde vom 12.-16. Oktober 2020. Die Prüfung erfolgte anhand von Dokumentensichtung und -prüfung, Interviews mit fachkundigem Personal, Ortsbesichtigung und Prüfung von Abläufen im Test- und Produktivsystem. Die Gutachtenerstellung wurde am 07. Januar 2021 abgeschlossen. Gegenstand der Prüfung waren neben dem Vorhandensein und dem Inhalt von Konzepten zum datenschutzgerechten Betrieb insbesondere die Überprüfung der Umsetzung am De-Mail-Produktivsystem mit besonderem Fokus auf der Einhaltung datenschutzrechtlicher Anforderungen.

Die datenschutzrechtliche Prüfung wurde auf Grundlage des De-Mail-Kriterienkataloges in der Version 2.1, der einschlägigen gesetzlichen Grundlagen sowie aufgrund der Technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) TR 01201 in der Version 1.6 durchgeführt. Der datenschutzrechtliche Rahmen ergibt sich aus der EU-Datenschutzgrundverordnung (DSGVO) sowie dem De-Mail-Gesetz und dem Bundesdatenschutzgesetz (BDSG).

B. Hintergrund

Das am 03. Mai 2011 in Kraft getretene De-Mail-Gesetz definiert De-Mail-Dienste in § 1 Abs. 1 als Dienste auf einer elektronischen Kommunikationsplattform, die einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen sollen.

De-Mail-Dienste dürfen nur von solchen Diensteanbietern betrieben werden, die nach dem De-Mail-Gesetz akkreditiert worden sind. Dazu muss der Diensteanbieter bestimmte Anforderungen erfüllen, wozu unter anderem die Einhaltung technischer und organisatorischer Maßnahmen nach der Technischen Richtlinie des BSI TR 01201 und datenschutzrechtliche Anforderungen gehören.

Die FP Digital Business Solutions GmbH bietet den De-Mail-Dienst nunmehr seit etwa 9 Jahren an. Entsprechend möchte sie die Akkreditierung gemäß § 17 Abs. 3 De-Mail-Gesetz erneuern.

Diesem Kurzgutachten liegt ein vom Prüfer erstelltes ausführliches Gutachten zugrunde, welches die Ergebnisse der Prüfung zur Erfüllung der datenschutzrechtlichen Anforderungen nach § 18 Abs. 3 Nr. 4 De-Mail-Gesetz dokumentiert. Auf Grundlage dieses Gutachtens wurde

der FP Digital Business Solutions GmbH durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) das für die Akkreditierung erforderliche Datenschutzzertifikat erteilt. Dieses Zertifikat bestätigt die Datenschutzkonformität der bei der FP Digital Business Solutions GmbH betriebenen De-Mail-Dienste. Die (Re-)Akkreditierung erfolgt am 06.03.2021.

Die Veröffentlichung dieses Kurzgutachtens soll Transparenz für potentielle Nutzer erzeugen sowie darüber informieren, wie die De-Mail funktioniert, was das Gesetz im Hinblick auf den Datenschutz vorschreibt, wie diese Vorgaben bei der FP Digital Business Solutions GmbH umgesetzt worden sind und dass der BfDI mit der Erteilung des Zertifikates das Verfahren für datenschutzkonform befunden hat.

Die FP Digital Business Solutions GmbH bietet als wählbare Dienste den Postfach- und Versanddienst, den öffentlichen Verzeichnisdienst und das Accountmanagement an. Darüberhinausgehende freiwillige Dienste wie die Dokumentenablage und ein Identitätsbestätigungsdienst sind nicht im Leistungsangebot enthalten.

C. Gegenstand und Ergebnisse der Prüfung

I. Funktionsweise von De-Mail

Die De-Mail ist ein eigenes Kommunikationsmittel, dass eine sichere, vertrauliche und nachweisbare Kommunikation im Internet für Bürger, öffentliche Stellen und nicht-öffentliche Stellen ermöglicht. Die De-Mail-Infrastruktur basiert auf E-Mail-Technik, fügt dieser aber weitere Merkmale hinzu, um eine sichere und verbindliche Kommunikation zu gewährleisten. Neben der Nachweismöglichkeit über die Identität der Kommunikationspartner sowie der Zustellung der De-Mails stellt der Dienst sicher, dass Inhalte von De-Mails auf ihrem Weg durch das Internet nicht mitgelesen oder manipuliert werden können.

De-Mail wird jedoch nur von geprüften und akkreditierten De-Mail-Providern angeboten.

Privatkunden können De-Mail über ein Webfrontend in gleicher Weise benutzen wie Webmail-Dienste. Der Zugriff auf De-Mail über das Internet ist nach dem Stand der Technik verschlüsselt (https, TLS). Bei Geschäftskunden erfolgt die Kommunikation über eine direkte Schnittstelle zu den Systemen der FP Digital Business Solutions GmbH.

De-Mail bietet die Möglichkeit, Eingangs-, Versand- und (in bestimmten Fällen) Abholbestätigungen anzufordern. Die Anmeldung kann wahlweise auf einer „normalen" Sicherheitsstufe mit Benutzername und Passwort oder auf einer „hohen" Sicherheitsstufe erfolgen. Bei der hohen Sicherheitsstufe wird neben Wissen (Passwort) als weiteres Authentizifierungsmittel auch Besitz gefordert. Hierfür stellt die FP Digital Business Solutions GmbH verschiedene Varianten zur Auswahl (neuer Personalausweis, qualifizierte Signaturkarte, Hardwaretoken, Mobil-TAN-Verfahren oder ein Gateway-Token).

II. Gesetzliche Anforderungen und Prüfprogramm

De-Mail-Anbieter unterliegen bei der Verarbeitung personenbezogener Daten der EU-Datenschutzgrundverordnung (DSGVO), dem Bundesdatenschutzgesetz (BDSG), dem De-Mail-Gesetz und dem Telemediengesetz (TMG). Der Kriterienkatalog des BfDI, der Grundlage des Gutachtens ist, schreibt die Prüfung der Einhaltung dieser gesetzlichen Vorgaben insbesondere anhand folgender Prüfungspunkte vor:

- Rechtmäßigkeit der Datenverarbeitung (Rechtsgrundlage)
- Erforderlichkeit und Zweckbindung
- Aufbewahrungsfristen und Löschung nach Wegfall der Erforderlichkeit
- Ordnungsgemäßer Einsatz von Auftragsverarbeitern
- Ordnungsgemäße Aufklärung und Information
- Beachtung datenschutzrechtlicher Anforderungen des De-Mail-Gesetzes
- Betroffenenrechte
- Sicherheit der Verarbeitung

Die Betroffenenrechte umfassen die in Kapitel III der DSGVO festgelegten Reche auf Transparenz, Auskunft, Berichtigung, Löschung, das Widerspruchsrecht und das Recht auf Datenübertragbarkeit. Die Sicherheit der Verarbeitung umfasst die Einhaltung der technischen und organisatorischen Anforderungen nach Art. 32 DSGVO, einschließlich der Anforderungen an die Verschlüsselung, die Authentifizierung und die Verwendung von Signaturen. Ferner war das Datenschutzmanagement, welches die Umsetzung der rechtlichen und technischen Vorschriften des Datenschutzes im laufenden Betrieb unter Einbeziehung des Datenschutzbeauftragten umfasst und sicherstellt, Gegenstand der Prüfung.

Die genannten Themenbereiche wurden für jeden der vom De-Mail-Anbieter angebotenen Dienste begutachtet. Im Fall der FP Digital Business Solutions GmbH wurden somit das Accountmanagement, der Postfach- und Versanddienst sowie der öffentliche Verzeichnisdienst geprüft.

III. Umsetzung bei der FP Digital Business Solutions GmbH

Die FP Digital Business Solutions GmbH hat die datenschutzrechtlichen Vorgaben im Rahmen des De-Mail-Dienstes in geeigneter und angemessener Weise umgesetzt. Die Anforderungen des Prüfkriterienkatalogs des BfDI sind erfüllt.

1. Account-Eröffnung und Verwaltung des De-Mail-Kontos

Bei der Account-Eröffnung und bei der Verwaltung des De-Mail-Kontos ist sichergestellt, dass personenbezogene Daten rechtmäßig erhoben werden, und zwar insbesondere auf Grundlage des Nutzungsvertrags über den De-Mail-Dienst sowie auf Grundlage des De-Mail-Gesetzes. Soweit Daten auf Grundlage einer Einwilligung erhoben werden, ist sichergestellt, dass die Einwilligung informiert und freiwillig erfolgt.

Die Daten werden ferner zweckgebunden erhoben und die Erhebung ist auf das erforderliche Maß beschränkt. Insbesondere werden Daten zur Identitätsfeststellung, Kontodaten, Kontaktdaten, Nutzungsdaten, Abrechnungsdaten, Protokolldaten und Dokumentationsdaten in rechtmäßiger Weise erhoben und verarbeitet. Dies gilt jeweils für die Benutzung des Dienstes durch natürliche Personen wie auch durch juristische Personen.

Die Aufbewahrungsfristen entsprechen den gesetzlichen Vorgaben (insbesondere § 13 De-Mail-Gesetz). Eine ordnungsgemäße Löschung entsprechend dem Stand der Technik nach Ende der Aufbewahrungsfrist ist sichergestellt.

Der Einsatz von Auftragsverarbeitern erfolgt gemäß den Vorgaben der DSGVO. Die Auftragsverarbeiter werden regelmäßig auf die Einhaltung der vertraglichen Verpflichtungen und der datenschutzrechtlichen Anforderungen geprüft.

Die FP Digital Business Solutions GmbH stellt den Nutzern die erforderlichen Informationen nach dem De-Mail-Gesetz und der DSGVO zur Verfügung. Für die

Ausübung der Betroffenenrechte gibt es angemessene Prozesse unter Einbindung des betrieblichen Datenschutzbeauftragten der FP Digital Business Solutions GmbH.

Die Identitätsprüfung der Nutzer bei der Registrierung sowie die Authentifizierung bei der Anmeldung zur Verwendung des Dienstes entsprechen dem Stand der Technik und gewährleisten die sichere Zuordnung der De-Mail-Adressen zu den registrierten Personen. Die Verbindung mit dem Nutzer ist nach dem Stand der Technik verschlüsselt. Die technisch-organisatorischen Sicherheitsmaßnahmen gewährleisten die Datensicherheit und die Einhaltung der gesetzlichen Vorschriften in angemessener Weise.

2. Postfach- und Versanddienst

Die Datenverarbeitung im Rahmen des Postfach- und Versanddienstes entspricht gleichfalls den Anforderungen des Datenschutzrechts. Insbesondere richtet sich die Verarbeitung der Nutzungsdaten, Verkehrsdaten und Protokolldaten nach den einschlägigen Vorschriften.

Die Grundsätze der Datensparsamkeit und der Zweckbindung sind gewahrt. Gemäß der Nutzungsvereinbarung übermittelt die FP Digital Business Solutions GmbH versendete De-Mails an den De-Mail-Provider des Empfängers. Hierbei werden neben der Nachricht nur die erforderlichen Protokoll- und Signaturinformationen übermittelt. Die empfangenden De-Mail-Provider sind gesetzlich zur zweckgebundenen Verwendung der Daten verpflichtet.

Die Vertraulichkeit, Integrität und Authentizität der De-Mail-Nachrichten ist gewährleistet durch eine Transportverschlüsselung sowie durch eine Inhaltsverschlüsselung der Nachrichten bei der Übermittlung zwischen den De-Mail-Providern.

Der De-Mail-Dienst der FP Digital Business Solutions GmbH bietet gemäß den Vorgaben des De-Mail-Gesetzes die Möglichkeit einer sicheren Anmeldung (mit zusätzlichem Authentifizierungsfaktor) und die Möglichkeit, dass der Versender einer Nachricht festlegt, dass diese vom Empfänger nur bei Verwendung der sicheren Anmeldung abgerufen werden kann (Versandoption „persönlich“). Alle Nachrichten und Bestätigungen werden entsprechend der Vorgaben der technischen Richtlinien (TR 01201) elektronisch signiert.

Die etablierten Verfahren und Prozesse gewährleisten eine den gesetzlichen Anforderungen entsprechende sichere Löschung nach Ablauf der Aufbewahrungsfristen entsprechend dem Stand der Technik.

Die Malwareprüfung und die sonstigen eingesetzten technischen Sicherheitsmaßnahmen entsprechen den gesetzlichen Anforderungen.

3. Verzeichnisdienst

Der Verzeichnisdienst ermöglicht eine Suche nach Inhabern von De-Mail-Adressen und ermöglicht umgekehrt den Nutzern, in das Verzeichnis aufgenommen zu werden. Die hierfür zu verwendenden Daten sind im De-Mail-Gesetz vorgegeben, die Veröffentlichung erfolgt auf freiwilliger Basis.

Die Grundsätze der Datenverarbeitung (insbesondere Rechtmäßigkeit, Datenminimierung, Speicherbegrenzung, Zweckbindung) sind eingehalten.

4. Betroffenenrechte

Die FP Digital Business Solutions GmbH hat angemessene und wirksame Prozesse, um die Rechte der Betroffenen nach Kapitel III der DSGVO auf Auskunft, Berichtigung, Löschung, Vergessenwerden, Einschränkung der Verarbeitung, Datenübertragbarkeit sowie auf Widerspruch gegen die Verarbeitung umzusetzen. Die Prozesse sehen dabei auch die Prüfung vor, ob die Voraussetzungen des jeweils geltend gemachten Anspruchs im Einzelfall erfüllt sind.

5. Datenschutzmanagement

Die Datenschutzorganisation der FP Digital Business Solutions GmbH gewährleistet die Einhaltung der datenschutzrechtlichen Anforderungen. Geprüft wurden insbesondere das Datenschutz- und IT-Sicherheitskonzept, die Rollen innerhalb der Datenschutzorganisation, das Schulungskonzept, die Datenschutzdokumentation und die etablierten Datenschutz-Prozesse.

IV. Zusammenfassung der Prüfungsergebnisse

Sämtliche geprüften Anforderungen des De-Mail-Kriterienkatalogs, der Datenschutzgrundverordnung, des Bundesdatenschutzgesetzes, des Telemediengesetzes, des De-

Mail-Gesetzes und des Signaturgesetzes sind erfüllt. Die von der FP Digital Business Solutions GmbH gewählten Maßnahmen sind geeignet, die datenschutzgerechte und sichere Verarbeitung personenbezogener Daten im Rahmen des De-Mail-Dienstes sicherzustellen. Dies gilt auch für die konkrete Umsetzung der Maßnahmen im laufenden Betrieb.

In der Gesamtbetrachtung liegt bei der FP Digital Business Solutions GmbH eine effiziente, durch den mittlerweile langjährigen Betrieb bewährte und vorbildliche Umsetzung der Datenschutzanforderungen vor. Die Mitarbeiter zeichnen sich durch eine hohe Sensibilisierung für den Datenschutz und den Schutz der Persönlichkeitsrechte der De-Mail-Nutzer aus. Die Implementierung des De-Mail-Dienstes entspricht funktional den strengen Vorgaben des De-Mail-Gesetzes und geht teilweise, insbesondere bei den gebotenen Alternativen für die sichere Anmeldung, sogar darüber hinaus.

D. Datenschutzfreundliche Ausgestaltung

Die FP Digital Business Solutions GmbH hat für den De-Mail-Dienst ein Datenschutzkonzept etabliert, dass die rechtlichen Vorgaben voll erfüllt und zum Teil erkennbar darüber hinausgeht. So werden durch das Angebot zusätzlicher Authentifizierungsmöglichkeiten für die sichere Anmeldung die technischen Möglichkeiten in nutzer- und datenschutzfreundlichem Sinn genutzt. Das Zugriffs- und Rollenkonzept bei der FP Digital Business Solutions GmbH ist detailliert und ermöglicht einen sehr wirksamen Zugriffsschutz. Die Sicherheitsmaßnahmen werden regelmäßig überprüft und dem Stand der Technik entsprechend fortentwickelt und angepasst.

***