Ronald Petrlic

Identitätsprüfung bei elektronischen Auskunftsersuchen nach Art. 15 DSGVO

Wie die Betroffenenrechte der DSGVO nicht zum Bumerang für die Betroffenen werden

Die Stärkung der Betroffenenrechte durch die DSGVO ist eine gute Sache für die Betroffenen. Die Verantwortlichen stellt der Umgang mit Auskunftsersuchen allerdings vor einige Herausforderungen – wie wir in Beratungsanfragen vermehrt feststellen. Vor allem in Bezug auf die Identitätsprüfung der antragstellenden Betroffenen gibt es Unklarheiten. Das Ziel dieses Beitrags ist es, unterschiedliche Maßnahmen zur Identitätsprüfung aufzuzeigen und gegenüberzustellen. Außerdem soll der Beitrag einen ersten Schritt zur Diskussion der Thematik darstellen. Bislang wurde dieses Thema bedauerlicherweise vernachlässigt. Die Konsequenzen einer mangelnden Umsetzung können für Betroffene doch beträchtlich sein.

1 Einführung

Mit der Datenschutzgrundverordnung (DSGVO) wurden die Rechte der von Datenverarbeitungen betroffenen Personen gestärkt. Neben dem bereits aus dem „alten" Datenschutzrecht bekannten Auskunftsrecht (nunmehr Artikel 15), dem Recht auf Berichtigung (Artikel 16), dem Recht auf Löschung bzw. „Recht auf Vergessenwerden" (Artikel 17) und dem Recht auf Einschränkung der Verarbeitung (Artikel 18) hat insbesondere das Recht auf Datenübertragbarkeit (Artikel 20) neu durch die DSGVO Einzug gehalten.

In Artikel 12 werden die Modalitäten für die Ausübung der Rechte der betroffenen Person näher ausgeführt. Neben der schriftlichen und elektronischen Kommunikation sieht Absatz 1 auch eine mündliche Erteilung von Informationen vor – „sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde". In Absatz 3 wird gefordert, dass die betroffene Person nach Möglichkeit auf elektronischem Weg zu unterrichten ist, sofern sie den Antrag elektronisch stellt und sie nichts anderes angibt. Im Hinblick auf die Identifizierung der betroffenen Person, die von ihren Betroffenenrechten Gebrauch machen möchte, regelt Absatz 6, dass der Verantwortliche zusätzliche Informationen anfordern kann, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

Dr. Ronald Petrlic

Referent beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

E-Mail: petrlic@lfdi.bwl.de

In diesem Beitrag wird exemplarisch auf das Auskunftsrecht der betroffenen Person eingegangen. Der Fokus liegt dabei auf der Fragestellung, wie der Verantwortliche mit einem Auskunftsersuchen einer betroffenen Person im Hinblick auf die Identitätsprüfung umzugehen hat. Die Überlegungen gelten dabei auch für die anderen erwähnten Betroffenenrechte.

Nach Artikel 15 Absatz 3 hat der Verantwortliche der betroffenen Person eine Kopie der personenbezogenen Daten zur Verfügung zu stellen, die Gegenstand der Verarbeitung sind. Dabei ist insbesondere auch vorgesehen, dass die betroffene Person den Antrag elektronisch stellen kann und ihr die Informationen auch in einem gängigen elektronischen Format zur Verfügung gestellt werden (Satz 3).

Bei den beim Verantwortlichen gespeicherten personenbezogenen Daten einer betroffenen Person kann es sich um sehr sensible Daten handeln. Eine Beauskunftung dieser Daten nach Artikel 15 an eine falsche Person kann unter Umständen gravierende Folgen für die betroffene Person nach sich ziehen; selbiges gilt für „Datenübertragungen" nach Artikel 20 an die falsche Person. Genauso gravierende Folgen kann ein gefälschter Antrag auf Berichtigung (Artikel 16), Antrag auf Löschung (Artikel 17) bzw. Antrag auf Einschränkung der Verarbeitung (Artikel 18) für die betroffene Person haben. Die eindeutige Identifizierung der betroffenen Person durch den Verantwortlichen vor der Durchführung der beantragten Maßnahmen ist daher von entscheidender Bedeutung.

In der Praxis gibt es sowohl seitens der Verantwortlichen als auch seitens der betroffenen Personen große Unsicherheiten, wie eine entsprechende Identifizierung ausgestaltet sein könnte und

darf. In der DSGVO finden sich keine Anhaltspunkte, welche „zusätzlichen Informationen“ zur Identifizierung herangezogen werden können. Auch das Kurzpapier Nr. 6 zum „Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO“ der Datenschutzkonferenz (DSK) gibt in diesem Punkt keine Antwort. Es wird lediglich festgehalten, dass „z. B. eine Postadresse bei elektronischem Auskunftsantrag“ nachgefordert werden kann. Beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) Baden-Württemberg häufen sich Anfragen von Verantwortlichen, welche Methoden der Identifizierung genutzt werden sollen und dürfen. Lassen Verantwortliche die betroffenen Personen eine Kopie eines Ausweisdokuments vorzeigen, stößt dies wiederum häufig auf Widerstand.

2 Wege der Antragstellung

Betroffene Personen können auf unterschiedlichen Wegen ein Auskunftsersuchen beim Verantwortlichen einreichen. Diese Wege skizzieren wir in diesem Abschnitt, bevor wir im nächsten Abschnitt näher darauf eingehen werden, wie eine Identifizierung der betroffenen Person ausgestaltet werden könnte.

2.1 Schriftlicher Antrag

Ein schriftlicher Antrag auf Auskunftsersuchen war bisher in der Praxis der wohl am häufigsten genutzte Weg um mit der verantwortlichen Stelle in Kontakt zu treten. Dies ist auch der Weg, den der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) auf seiner Website empfiehlt [1]. Die Auskunft wird in diesem Fall typischerweise auch schriftlich an die im Antrag angegebene Anschrift erfolgen.

2.2 Telefonischer Antrag

Wie bereits eingangs erwähnt sieht Artikel 12 Absatz 1 DSGVO auch eine mündliche Erteilung von Informationen vor. Es ist also denkbar, dass betroffene Personen ein Auskunftsersuchen per Telefon stellen.

2.3 Antrag per E-Mail

Das Auskunftsersuchen per E-Mail zu stellen ist aus Sicht der betroffenen Person vermutlich der einfachste Weg. Dies scheint – laut Anfragen, die uns von damit konfrontierten Verantwortlichen vorliegen – auch der zurzeit bevorzugte Weg zu sein.

Im Hinblick auf die Identifizierung der betroffenen Person stellt eine Antragstellung per E-Mail für den Verantwortlichen allerdings eine große Herausforderung dar. Sofern die E-Mail-Adresse dem Verantwortlichen noch nicht bekannt ist, lässt sich aus der E-Mail-Adresse keinesfalls auf die wahre Identität der betroffenen Person schließen. Aus der Aufsichtspraxis sind uns zudem auch aus der Vergangenheit viele Fälle bekannt, bei denen betroffene Personen unter einer anderen E-Mail-Adresse Anfragen an den Verantwortlichen richten, als die E-Mail-Adresse in deren Stammdatensatz beim Verantwortlichen vorliegt.

2.4 Antrag über Website (Nutzerkonto)

Sollte die betroffene Person bereits ein Nutzerkonto auf der Website des Verantwortlichen haben, so ist auch die Antragstellung über dieses Nutzerkonto denkbar. So wird dies etwa schon seit längerer Zeit bei sozialen Netzwerken gehandhabt. Je nach Umfang der Daten können diese der betroffenen Person direkt zur Verfügung gestellt werden, oder es ist auch denkbar, dass die betroffene Person nach erfolgter Antragstellung einen Hinweis (bspw. per E-Mail) erhält, dass die Auskunft nun über das Nutzerkonto abgeholt werden kann.

Neben den besprochenen Antragswegen sind natürlich weitere denkbar, die hier nicht weiter diskutiert werden – etwa ein persönlicher Antrag vor Ort beim Verantwortlichen, der im Hinblick auf die Identifizierung keine Probleme darstellen sollte, in den meisten Fällen aber wahrscheinlich eher nicht praktikabel sein wird.

3 Methoden der Identifizierung

Die skizzierten Antragswege stellen im Hinblick auf die Identifizierung der antragstellenden, betroffenen Person unterschiedliche Herausforderungen; diese sollen in diesem Abschnitt näher diskutiert werden. Dazu werden mögliche Methoden der Identifizierung[1] vorgestellt.

3.1 Abfrage von zusätzlichen Informationen

Bei telefonischen Anfragen ist es – auch in anderen Kontexten, bspw. bei Fragen zu Verträgen – gängige Praxis, dass der Verantwortliche von der betroffenen Person zusätzliche Informationen abfragt, um sicherzugehen, dass es sich tatsächlich um die richtige Person handelt. Typischerweise handelt es sich dabei um Daten wie Geburtsdatum und Anschrift der betroffenen Person. In wenigen Fällen (fast ausschließlich beim Telebanking) werden „richtige“ Geheimnisse (etwa eine zuvor mitgeteilte PIN) abgefragt.

3.2 Übermittlung eines Ausweisdokuments

Um missbräuchliche Auskunftsbegehren zu verhindern, sieht der BfDI die Vorlage eines Personaldokuments zur Legitimation (in Einzelfällen) als zulässig an. Von der Ausweiskopie werden „regelmäßig nur Name, Anschrift, Geburtsdatum und Gültigkeitsdauer benötigt“ und alle anderen Daten können auf der Kopie grundsätzlich geschwärzt werden, wie der BfDI weiter ausführt [1].

Bei der postalischen Übermittlung einer geschwärzten Ausweiskopie gibt es aus Datenschutzsicht keine allzu großen Bedenken. Selbstverständlich ist, dass die Daten auf der Ausweiskopie einer strengen Zweckbindung unterliegen und ausschließlich zur Identitätsprüfung verwendet werden, nicht aber in den Datenbestand der verantwortlichen Stelle einfließen dürfen [1].

Eine Übermittlung einer geschwärzten Ausweiskopie per E-Mail ist aus Datenschutzsicht schon bedenklicher. Stellt die betroffene Person den Antrag per E-Mail und fordert der Verantwortliche die Zusendung einer Ausweiskopie, so hat der Ver-

1 Der Einfachheit halber sprechen wir hier nur von „Identifizierung“, auch wenn man streng genommen von Identifizierung und Authentifizierung sprechen müsste.

antwortliche hierfür einen sicheren Zugangsweg bereitzustellen. In Frage kommt bspw. die Bereitstellung eines öffentlichen Schlüssels des Verantwortlichen, mit dem die betroffene Person die Ausweiskopie Ende-zu-Ende-verschlüsselt per E-Mail übermitteln kann. Als nutzerfreundlichere Alternative – im Hinblick auf die geringe Nutzung von Ende-zu-Ende-Verschlüsselung – kommt hierfür etwa auch die Bereitstellung eines Links zu einer HTTPS-geschützten Website in Betracht, über die die betroffene Person die Ausweiskopie (ohne weitere selbst zu ergreifende Maßnahmen) sicher an den Verantwortlichen übermitteln kann.

3.3 Identifizierung über eIDAS-Dienst

Die eIDAS-Verordnung [2] aus dem Jahr 2014 hat zum Ziel, das Vertrauen in elektronische Transaktionen im Binnenmarkt zu stärken, indem eine „gemeinsame Grundlage für eine sichere elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen geschaffen wird". Die eIDAS-Verordnung enthält verbindliche europaweit geltende Regelungen zur elektronischen Identifizierung und zu elektronischen Vertrauensdiensten. [3]

In Deutschland und den anderen EU-Mitgliedsstaaten wurden bereits elektronische Identifizierungssysteme und Vertrauensdienste eingeführt, die der eIDAS-Verordnung entsprechen. Für Deutschland sind hier insbesondere die Online-Ausweisfunktion des elektronischen Personalausweises sowie De-Mail zu nennen, die für eine sichere Identifizierung von betroffenen Personen genutzt werden können. Daneben kommt hierfür auch die qualifizierte elektronische Signatur in Frage. Bei all diesen Verfahren wurde die Identität der betroffenen Person im Vorhinein durch eine vertrauenswürdige Stelle eindeutig geprüft; darauf können sich die Verantwortlichen stützen.

Im Detail unterscheiden sich die Verfahren dennoch. Mit der Online-Ausweisfunktion des Personalausweises lässt sich etwa das Geburtsdatum (und gegebenenfalls auch die Anschrift) mit in den Identifizierungsprozess des Verantwortlichen aufnehmen, um Verwechslungen bei Namensgleichheit von betroffenen Personen auszuschließen. Eine bestätigte E-Mail-Adresse der betroffenen Person fehlt allerdings. Stellt eine betroffene Person einen Antrag über De-Mail, kann der Verantwortliche sicher sein, dass die De-Mail-Adresse tatsächlich zu der (geprüften) Identität der betroffenen Person gehört. Weitergehende (von einer vertrauenswürdigen Stelle bestätigte) Identifizierungsmerkmale wie Geburtsdatum oder Anschrift fehlen allerdings. Dasselbe gilt für einen eingehenden Antrag per E-Mail, der mit einer qualifizierten elektronischen Signatur versehen ist.

3.4 Post-/Video-Ident-Identifizierung

Das Postident (durch Postfiliale)-Verfahren der Deutschen Post dürfte Vielen bereits bekannt und vertraut sein. Bei diesem Verfahren wird die persönliche Identifizierung durch einen Mitarbeiter der Deutschen Post vorgenommen, etwa nach einer online beantragten Eröffnung eines Bankkontos oder der Bestellung einer SIM-Karte. Der Post-Mitarbeiter prüft dabei den Ausweis des anwesenden Antragstellers, fertigt eine Kopie davon an und leitet die Bestätigung der Identitätsfeststellung an den Verantwortlichen weiter, der die Identitätsfeststellung in Auftrag gegeben hat.

Als Weiterentwicklung zum „klassischen" Postident-Verfahren haben sich in den letzten Jahren auch Postident-Verfahren durch Videochat am Markt etabliert.[2] Dabei muss keine Post-Filiale mehr aufgesucht werden, sondern die Identifizierung findet per Videochat mit einem Mitarbeiter des Identifizierungsdiensteanbieters statt. Dabei werden Aufnahmen der betroffenen Person und des Ausweises angefertigt.

Sowohl das klassische Postident-Verfahren als auch ein Video-Ident-Verfahren können für die Identifizierung von betroffenen Personen, die von ihrem Auskunftsrecht Gebrauch machen möchten, in Frage kommen. Die Identifizierung muss dabei nicht zwingend durch einen speziellen Identifizierungsdiensteanbieter, sondern könnte etwa auch durch den Verantwortlichen selbst (per Videochat) oder persönlich (in einer Filiale des Verantwortlichen vor Ort der betroffenen Person) durchgeführt werden.

3.5 Identifizierung über Nutzerkonto

Die Antragstellung der betroffenen Person nach erfolgreicher Identifizierung über ein bereits bestehendes Nutzerkonto beim Verantwortlichen ist vermutlich am einfachsten umzusetzen. Erwägungsgrund 57 (zu Artikel 11) DSGVO sieht insbesondere vor, dass die Identifizierung die „digitale Identifizierung einer betroffenen Person – beispielsweise durch Authentifizierungsverfahren etwa mit denselben Berechtigungsnachweisen, wie sie die betroffene Person verwendet, um sich bei dem von dem Verantwortlichen bereitgestellten Online-Dienst anzumelden" mit einschließt. Das bedeutet, dass wenn die betroffene Person ein Nutzerkonto bei dem Verantwortlichen hat, von ihm keine zusätzliche (über die Identifizierung und Authentifizierung über das Nutzerkonto hinausgehende) Identifizierung verlangt werden darf.

4 Bewertung der Identifizierungs-Methoden

Die aufgezeigten Identifizierungsverfahren bieten unterschiedliche Sicherheitsgarantien; auf die jeweiligen Vor- und Nachteile der Verfahren gehen wir in diesem Abschnitt näher ein.

4.1 Abfragen von zusätzlichen Informationen

Das Problem bei der heutzutage (in anderen Kontexten) bereits häufig genutzten telefonischen Identifizierung besteht darin, dass die abgefragten Informationen in der Regel keine richtigen Geheimnisse darstellen. Jeder, der die betroffene Person (deren Daten beauskunftet werden sollen) näher kennt – etwa Familienmitglieder, Freunde, Arbeitskollegen –, wird in der Lage sein, die Identifizierungsfragen zu beantworten. Sollen sensible personenbezogene Daten (insbesondere besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO bzw. Finanzdaten) beauskunftet werden, sollten Verantwortliche nicht auf diese Identifizierungsmethode zurückgreifen.

4.2 Übermittlung eines Ausweisdokuments

Die Übermittlung eines Ausweisdokuments (per Post oder über gesicherte E-Mail bzw. gesicherte Website) bringt eine höhere Sicherheit in Bezug auf die Sicherheit der Identifizierung. Ein Vorteil dieses Verfahrens aus Datenschutzsicht ist, dass der Ausweis

2 Video-Ident-Verfahren werden nicht nur durch die Deutsche Post AG angeboten, sondern auch durch andere Anbieter.

vor der Übermittlung geschwärzt werden kann; lediglich Name, Anschrift, Geburtsdatum und Gültigkeitsdauer werden für die Identifizierung benötigt. Die Antwort des Auskunftsersuchens geht in der Regel an die im Ausweisdokument angegebene Anschrift. Die Datenschutz-Aufsichtsbehörden haben bisher keine größeren Einwände gegen das Verfahren geäußert.

In Bezug auf die Vertraulichkeit des Antwortschreibens ist das Verfahren ohne Zweifel unproblematisch. Ein Aspekt, der aus Datenschutzsicht allerdings trotzdem bedacht werden sollte ist, dass der Verantwortliche nicht zweifelsfrei sicher sein kann, dass das Auskunftsersuchen tatsächlich vom Inhaber des Ausweisdokuments gestellt wurde. Es ist denkbar, dass etwa Familienmitglieder oder WG-Mitbewohner, die Zugang zum Ausweis der betroffenen Person (sowie Zugang zur Eingangspost[3]) haben, das Auskunftsersuchen im Namen der betroffenen Person stellen. Gerade im Hinblick auf Dienste wie etwa Partnersuchbörsen könnte eine Auskunft an eine andere im selben Haushalt lebende Person Konsequenzen für die betroffene Person nach sich ziehen. Über das Auskunftsrecht bestünde somit die potentielle Möglichkeit, in Erfahrung zu bringen, welche Dienste Ehepartner oder Kinder nutzen.

4.3 Identifizierung über eIDAS-Dienst

Im Gegensatz zur Übermittlung eines Ausweisdokuments zur Identifizierung ist bei der Identifizierung über einen eIDAS-Dienst eine stärkere Authentifizierung der betroffenen Person nötig. Bei der Nutzung der Online-Ausweisfunktion des Personalausweises muss der Antragsteller nicht nur im Besitz des Ausweises sein, sondern zusätzlich auch noch die PIN kennen, um sich erfolgreich zu identifizieren (und zu authentifizieren).

Der Vorteil dieser Identifizierungsmethode ist, dass sich die betroffene Person nur einmal zu Beginn (bei Beantragung des Identifizierungsdiensts) physisch identifizieren muss und den Dienst später europaweit nutzen kann. Dienste nach der eIDAS-Verordnung werden heutzutage von Bürgern allerdings noch nicht in größerem Umfang genutzt.

4.4 Post-/Video-Ident-Identifizierung

Die Post-/Video-Ident-Identifizierung weist im Gegensatz zu den bisher besprochenen Verfahren die höchste Sicherheit in Bezug auf die Identifizierung auf. Bei dem Verfahren ist sichergestellt, dass tatsächlich die betroffene Person das Auskunftsersuchen stellt; die betroffene Person muss sich persönlich mit ihrem gültigen Ausweisdokument bei einer vertrauenswürdigen Stelle identifizieren. Aus Datenschutzsicht weniger schön ist, dass eine Schwärzung der Kopie (bzw. Videoaufnahme) des Ausweisdokuments nicht möglich ist. Bei der Nutzung von Postident (durch einen Mitarbeiter einer Postfiliale) erfolgt laut Datenschutzbestimmungen[4] der Deutschen Post AG keine dauerhafte Speicherung der Daten bei der Post. Fraglich ist, ob datenschutzbewusste Bürger bereit sind, eine Video-Ident-Identifizierung durchzuführen. In jedem Fall sollten die Datenschutzbestimmungen des jeweiligen Identifizierungsdienstleisters genau geprüft werden. Bei der Deutschen Post AG ist es beispielsweise so, dass beim Post-ident-Verfahren durch Videochat „je nach Verfahren" die Aufzeichnung (Audio und Video) des gesamten Identifizierungsprozesses an den Verantwortlichen weitergeleitet werden.

Die hohe Sicherheit dieses Identifizierungsverfahrens geht zudem mit einem hohen Aufwand für die betroffene Person einher.

4.5 Identifizierung über Nutzerkonto

Die Sicherheit des Identifizierungsverfahrens hängt bei dieser Methode sehr stark von dem vom Nutzer vergebenen Passwort für sein Nutzerkonto ab. Gerade für Nutzer, die keine starken Passwörter verwenden, können sich die Betroffenenrechte bei diesem Verfahren als Bumerang erweisen. Jemand, der sich Zugang zum Nutzerkonto der betroffenen Person verschafft, kann über die Ausübung der Betroffenenrechte (neben dem Auskunftsrecht denke man hier auch an die anderen eingangs erwähnten Rechte) einigen Schaden anrichten. Wünschenswert wäre, dass zur Ausübung der Betroffenenrechte über das Nutzerkonto eine Zwei-Faktor-Authentifizierung nötig ist.

In Bezug auf den Aufwand für die Identifizierung im Rahmen der Beantragung des Auskunftsersuchens stellt dieses Verfahren sowohl für die betroffene Person als auch für den Verantwortlichen die einfachste Form dar.

4.6 Auswahl des passenden Verfahren

Die schlechte Nachricht vorweg: Verantwortliche müssen selbst entscheiden, welche Identifizierungsmethode sie für Auskunftsersuchen von betroffenen Personen wählen; und zwar – und das dürfte auch keine große Überraschung sein – unter Berücksichtigung des Risikos für die Rechte und Freiheiten der betroffenen Personen. In diesem Kontext sei insbesondere auf Artikel 32 DSGVO hingewiesen. Betrachten wir den Prozess der Auskunftserteilung als Verarbeitung im Sinne der DSGVO, so ist nach Erwägungsgrund 83 ein Schutzniveau (auch hinsichtlich der Vertraulichkeit) zu gewährleisten, das „den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist." Bei der Ermittlung des Risikos sollen nach Erwägungsgrund 83 „Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von oder unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden" mit berücksichtigt werden. Alle diese Probleme können bei unsachgemäßer Umsetzung der Prozesse zur Umsetzung der Betroffenenrechte auftreten.

Aus dem Beitrag sollte hervorgegangen sein, dass in Fällen, bei denen es um sehr sensible personenbezogene Daten bzw. große Datenmengen geht (Stichwort Datenübertragbarkeit), sichere Identifizierungsverfahren zum Einsatz kommen sollten. Dasselbe gilt in Fällen, bei denen allein schon die Nutzung eines Dienstes anderen Personen nicht offengelegt werden sollte.

Gleichzeitig sollte klar geworden sein, dass sichere Identifizierungsverfahren insbesondere auch im Sinne der betroffenen Personen liegen sollten; auch wenn der Aufwand für die Identifizierung je nach Schutzniveau für die betroffenen Personen beträchtlich sein kann.

Selbstverständlich dürfen die für den Zweck der Identifizierung zusätzlich erhobenen personenbezogenen Daten vom Verantwortlichen nicht für andere Zwecke verwendet werden. Die Angst vieler Nutzer, dass dies doch passieren könnte, zeigt sich u. a. an der geringen Akzeptanz für die Zwei-Faktor-Authenti-

3 Würde der Antragsteller eine Antwort per E-Mail wünschen, wäre kein Zugang zur Eingangspost nötig.

4 https://www.deutschepost.de/content/dam/dpag/html/ext/postid/Datenschutzhinweise.pdf

fizierung[5] – die aus Sicherheitssicht einen großen Nutzen für die Nutzer bringen würde.

4.7 Antwort an die betroffene Person

Das Hauptaugenmerk in diesem Beitrag lag auf der Identifizierung von betroffenen Personen, die ein Auskunftsersuchen beim Verantwortlichen beantragen. Genauso wichtig ist natürlich die Frage, auf welchem Wege die Auskunft schließlich erteilt wird; wenn die Auskunft nicht schriftlich per Post erfolgt.

Hierzu lässt sich ebenfalls wieder festhalten, dass ein dem Schutzniveau angemessener Weg gefunden werden muss. Eine Übermittlung personenbezogener Daten per „normaler" (nicht-Ende-zu-Ende-verschlüsselter) E-Mail ist aus Datenschutzsicht problematisch (aber nicht in allen Fällen verboten). Sensible personenbezogene Daten dürfen hingegen nicht ohne Ende-zu-Ende-Verschlüsselung beauskunftet werden. Falls – was in den meisten Fällen der Fall sein wird – die betroffene Person keinen öffentlichen Schlüssel bereitstellt[6], mittels dessen die E-Mail vom Verantwortlichen an die betroffene Person verschlüsselt werden könnte, sind andere Wege zu suchen. Denkbar ist etwa die Übermittlung eines verschlüsselten PDF-Dokuments, wobei das zum Öffnen des Dokuments nötige Passwort über einen vertrauenswürdigen Kanal mitgeteilt werden muss. Einfacher gestaltet es sich, wenn das Auskunftsersuchen per De-Mail eingegangen ist. In diesem Fall ist es möglich, ohne zusätzliche Ende-zu-Ende-Verschlüsselung auch sensible personenbezogene Daten per De-Mail zu beauskunften. Die Bereitstellung der Auskunft über das (https-gesicherte) Nutzerkonto ist wiederum die einfachste Möglichkeit.

5 Damit verbunden die Weitergabe der Telefonnummer an den Diensteanbieter.

6 Etwa im Rahmen der Identifizierung mittels E-Mail mit qualifizierter elektronischer Signatur (nach eIDAS-Verordnung).

5 Zusammenfassung und Ausblick

Die Stärkung der Betroffenenrechte durch die DSGVO ist eine gute Sache. Betroffene Personen nehmen auch vermehrt ihre Rechte wahr. Verantwortliche stellt dies allerdings vor nicht zu unterschätzende Herausforderungen. Allein der Aspekt „Identifizierung" ist, wie wir in diesem Beitrag aufgezeigt haben, nicht ganz einfach umzusetzen. Einerseits gilt es für Verantwortliche einen Weg zu finden, um möglichst hohe Sicherheit im Identifizierungsprozess zu erhalten: Auskünfte an „falsche" Personen sollten weitestgehend vermieden werden. Andererseits sieht die DSGVO vor, dass das Wahrnehmen der Betroffenenrechte mit möglichst geringem Aufwand für die betroffenen Personen möglich ist. Bisher gibt es noch keine etablierten Verfahren zur Identifizierung, die sich durchgesetzt haben. Verantwortliche sind daher gut beraten, sich noch vor dem ersten Auskunftsersuchen Gedanken zur Umsetzung zu machen. Andernfalls steht zu befürchten, dass es in Zukunft vermehrt zu Missbrauch kommen wird: Eine mangelhafte Umsetzung könnte Betrügern das Abgreifen von personenbezogenen Daten leicht machen.

Literatur

[1] BfDI: *Recht auf Auskunft*, https://www.bfdi.bund.de/DE/Datenschutz/Ueberblick/MeineRechte/Artikel/Auskunftsrecht.html, zuletzt aufgerufen im September 2018.

[2] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rats vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

[3] BSI: *eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste*, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/eIDAS/eIDAS_node.html, zuletzt aufgerufen im September 2018.