Identitätsprüfung – welche Methoden gibt es?

Mit dem in Art. 15 DSGVO geregelten bedeutsamen Betroffenenrecht, dem Recht auf Auskunft, kann die betroffene Person Auskunft von den Unternehmen verlangen, welche personenbezogenen Daten von ihm verarbeitet wurden bzw. verarbeitet werden. Um von diesem Recht Gebrauch zu machen, braucht es keine vorgeschriebene Vorlage.

Bei den beim Verantwortlichen gespeicherten personenbezogenen Daten einer betroffenen Person kann es sich um sehr sensible Daten handeln, daher ist eine eindeutige Identifizierung der betroffenen Person durch den Verantwortlichen vor der Durchführung der beantragten Maßnahmen unabdingbar.

Wie kann der Verantwortliche die Identität mit einem Auskunftsersuchen einer betroffenen Person datenschutzkonform prüfen? Wir stellen die Vor- bzw. Nachteile der unterschiedlichen Verfahren gegenüber.

1. Wege der Antragstellung

Die Modalitäten für die Ausübung eines Auskunftersuchen sind in Art. 12 DSGVO geregelt. Auskunftsersuche der gespeicherten Daten könnten auf unterschiedlichen Wegen bei dem Verantwortlichen eingehen:

- **schriftlicher Antrag**, in der Praxis der wohl am meisten genutzte Weg, um mit der verantwortlichen Stelle in Kontakt zu treten.
- **telefonischer Antrag**, gemäß Art. 12 DSGVO ist auch eine mündliche Anfrage (per Telefon) auf Auskunft möglich.
- **Antrag per E-Mail**, aus Sicht der betroffenen Person vermutlich der einfachste Weg, welcher heutzutage wohl am häufigsten durchgeführt wird.
- **Antrag über Website (Nutzerkonto)**
- Auch eine Antragstellung über ein Nutzerkonto auf der Webseite des Verantwortlichen wäre denkbar.
- **Antrag direkt vor Ort**, jedoch in den meisten Fällen eher nicht praktikabel sein.

2. Methoden der Identifizierung

Wir stellen Ihnen mögliche Methoden zur Identifizierung vor, welche die antragstellenden, betroffenen Personen vor unterschiedliche Herausforderungen stellen.

Abfrage von zusätzlichen Informationen

Bei telefonischen Anfragen ist es gängige Praxis, dass der Verantwortliche von der betroffenen Person zusätzliche Informationen abfragt. Typischerweise handelt es sich dabei um Daten wie Geburtsdatum und Anschrift der betroffenen Person. Jedoch sind diese abgefragten Informationen in der Regel keine richtigen Geheimnisse. Jeder, der die betroffene Person 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 Gesundheits- bzw. Finanzdaten) beauskunftet werden, sollten Verantwortliche nicht auf diese Identifizierungsmethode zurückgreifen. Dann könnte eine zusätzliche Identifizierungsfrage z. B. eine individuelle PIN, eine Patienten- bzw. Kundennummer sein.

Übermittlung eines Ausweisdokuments

Um missbräuchliche Auskunftsbegehren zu verhindern, sieht der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die Vorlage eines Personaldokuments zur Legitimation nur in Einzelfällen als zulässig an. Jedoch sollte diese Variante nicht als erste Wahl zur Identifizierung herangezogen werden. Wird eine Kopie des Personalausweises an den Verantwortlichen gesendet, ist Vorsicht geboten. Es müssen bis auf Namen, Anschrift, Geburtsdatum und Gültigkeitsdauer alle sonstigen Ausweisdaten geschwärzt werden. Dies gebietet der Grundsatz der Datenminimierung. Der Grundsatz der Speicherbegrenzung gemäß Art. 5 Abs.1 lit. c und e DSGVO verlangt zudem, dass sofern die Ausweiskopie nicht mehr benötigt wird, diese unverzüglich nach Feststellung der erforderlichen Angaben gelöscht oder vernichtet wird. Ausnahmen hiervon können sich allenfalls aus spezialgesetzlichen Aufbewahrungsfristen ergeben. Wird die Ausweiskopie per Mail verschickt, muss der Verantwortliche zusätzlich darauf achten, dass ein sicherer Zugangsweg bereitgestellt wird.

Dennoch bleibt aber zu beachten, dass der Verantwortliche nicht zweifelsfrei sicher sein kann, dass das Auskunftsersuchen tatsächlich vom Inhaber des Ausweisdokuments gestellt wurde. Es wäre denkbar, dass etwa Familienmitglieder oder WG-Mitbewohner, die Zugang zum Ausweis der betroffenen Person (sowie Zugang zur Eingangspost) haben und das Auskunftsersuchen im Namen der betroffenen Person stellen. Über das Auskunftsrecht wäre es somit möglich, über Ehepartner oder Kinder in Erfahrung zu bringen, welche Dienste sie nutzen.

Identifizierung über eIDAS-Dienst

In 2014 wurde durch die eIDAS-Verordnung eine Online-Ausweisfunktion eingeführt. Dies sollte das Vertrauen in elektronische Transaktionen im Binnenmarkt stärken und außerdem eine gemeinsame Grundlage für eine sichere elektronische Interaktion zwischen Bürgern, Unternehmen und öffentlichen Verwaltungen schaffen. Die eIDAS-Verordnung enthält verbindliche europaweit geltende Regelungen zur elektronischen Identifizierung und zu elektronischen Vertrauensdiensten. 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 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.

Post-/Video-Ident-Identifizierung

Die Identifizierung muss dabei nicht zwingend durch einen speziellen Identifizierungsdiensteanbieter durchgeführt, sondern kann etwa auch durch den Verantwortlichen selbst (per Videochat) oder persönlich (in einer Filiale des Verantwortlichen vor Ort der betroffenen Person) durchgeführt werden. Es wird dabei jeweils der anwesende Antragsteller mit dem Lichtbild des Ausweises überprüft. Anschließend wird von dem Ausweis eine Kopie angefertigt und die Bestätigung der Identitätsfeststellung an den Verantwortlichen weitergeleitet, der die Identitätsfeststellung in Auftrag gegeben hat. Als Weiterentwicklung ist die Identitätsfeststellung nun auch per Videochat möglich. So muss keine Filiale mehr aufgesucht werden.

Die Post-/Video-Ident-Identifizierung weist im Gegensatz zu den bisher besprochenen Verfahren die höchste Sicherheit in Bezug auf die Identifizierung auf. Jedoch ist dieser Vorgang mit einem hohen Aufwand für die betroffene Person verbunden.

Aus Datenschutzsicht weniger schön ist, dass eine Schwärzung der Kopie (bzw. Videoaufnahme) des Ausweisdokuments nicht möglich ist. Je nach Identifizierungsdiensteanbieter wird teilweise der gesamte Identifizierungsprozesses an den Verantwortlichen weitergeleitet. Daher sollten datenschutzbewusste Bürger vorher die Datenschutzbestimmungen des jeweiligen Identifizierungsdienstleisters genau prüfen.

Identifizierung über Nutzerkonto

Die Antragstellung der betroffenen Person nach erfolgreicher Identifizierung über ein bereits bestehendes Nutzerkonto beim Verantwortlichen ist vermutlich am einfachsten umzusetzen und auch 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.

Auch eine gesicherte Übermittlung der angeforderten Auskunft wäre über das Nutzerkonto möglich. Es könnte nach erfolgter Antragstellung anschließend ein Hinweis (z. B. per Mail) an die betroffene Person übermittelt werden, dass die Auskunft über das Nutzerkonto abgerufen werden kann.

Es ist jedoch zu beachten, dass die Sicherheit des Identifizierungsverfahrens sehr stark von dem Nutzer vergebenen Passwort abhängt. Gerade wenn Nutzer keine starken Passwörter verwenden, kann dadurch schnell einiger Schaden angerichtet werden. Abhilfe könnte in einem solchen Fall nur eine Zwei-Faktor-Authentifizierung schaffen.

3. Auswahl des passenden Verfahrens

Unter Berücksichtigung des Risikos für die Rechte und Freiheiten der betroffenen Personen (Art. 32 DSGVO) bleibt es von dem Verantwortlichen abzuwägen, welche Identifizierungsmethode für das Auskunftsersuchen von den betroffenen Personen gefordert wird.

Besonders zu beachten ist, 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.

4. Antwort an die betroffene Person

Um die angefragten Daten an die betroffene Person zu übermitteln, muss dafür dem Schutzniveau angemessener Weg gefunden werden. Die Übermittlung personenbezogener Daten schriftlich per Post ist ein möglicher Weg. Weiter könnte ein verschlüsseltes PDF-Dokument verwendet werden, damit sensible personenbezogene Daten sicher übermittelt werden können.

Das zum Öffnen des Dokuments benötigte Passwort sollte separat über einen vertrauenswürdigen Kanal mitgeteilt werden. Auch eine Bereitstellung der Auskunft über ein (https-gesicherte) Nutzerkonto wäre möglich. Von einer Übermittlung der Anfrage in einer normalen und unverschlüsselten E-Mail ist jedoch abzuraten.

5. Zusammenfassung und Ausblick

Verantwortliche sollten sich bereits vor dem ersten Auskunftsersuchen Gedanken zur Umsetzung machen. Allein der Aspekt Identifizierung ist nicht ganz einfach umzusetzen. Einerseits gilt es für Verantwortliche einen Weg zu finden, um möglichst hohe Sicherheit im Identifizierungsprozess zu erhalten und dadurch Auskünfte an „falsche“ Personen zu vermeiden und andererseits, dass das Wahrnehmen der Betroffenenrechte mit möglichst geringem Aufwand für die betroffenen Personen möglich ist.

Bei Fragen stehen wir Ihnen jederzeit zur Verfügung.

Ihr Team der RKM Data GmbH