Betroffenenrechte: Identitätsnachweis bei Auskunftsersuchen

Stand: Februar 2019

Über den Autor

Daniel Steffen, Geschäftsführer der Digitalagentur novinet ist zertifizierter Datenschutzbeauftragter (DSB-TÜV) und Datenschutzauditor (DSA-TÜV) und berät deutschlandweit Unternehmen sowie Vereine und Agenturen im Umgang mit der Datenschutzgrundverordnung.

Mit Einzug der DSGVO wurden die Rechte der Betroffenen auf ein neues Niveau gehoben. Diverse Artikel der Grundverordnung widmen sich dem Recht auf Auskunft, Berichtigung oder Löschung von personenbezogenen Daten. Die Anträge der Betroffenen können dabei nicht nur schriftlich, sondern auch per E-Mail oder Telefon gestellt werden.

Identität des Betroffenen muss festgestellt werden

An dieser Stelle stehen Unternehmen oftmals vor dem ersten Problem: wie kann die Identität des Antragstellers zweifelsfrei sichergestellt werden? Das Zusenden personenbezogener Daten an einen unberechtigten Dritten stellt nämlich selbst schon einen Verstoß gegen die DSGVO dar. Dies wird dadurch erschwert, dass vom Betroffenen für die Identifizierung bereitgestellten Daten von den im System der Unternehmen gespeicherten Daten abweichen können. So entspricht die E-Mail-Adresse des Antragstellers nicht der im System hinterlegten, die postalische Adresse hat sich durch einen Umzug geändert oder der Anrufer ruft aus dem Büro und entsprechend mit der Telefonnummer des Arbeitgebers an.

Grundsätzliches bei Betroffenenanfragen

- Ein Antrag muss stets beantwortet werden. Auch sog. Negativauskünfte müssen gegeben werden
- Für die Bearbeitung eines Antrags hat das Unternehmen grundsätzlich maximal 30 Tage Zeit
- Alle Auskünfte (sowie die damit verbundene Kommunikation) sollten dokumentiert werden
- Die Beantwortung eines Antrags sollte grundsätzlich an die im System gespeicherte Adresse verschickt werden. Abweichende Adressen bedürfen einer erneuten Identitätsprüfung
- Die Identität der betroffenen Person sollte zweifelsfrei sichergestellt werden. Dabei sollte auch stets der zumutbare Aufwand für den Betroffenen im Verhältnis zu der Kritikalität der Daten beachtet werden

Möglichkeiten der Identifizierung einer betroffenen Person

Antragsteller identisch mit gespeicherten Daten
Sofern sich die Angaben des Antragstellers mit den im Unternehmen gespeicherten Daten decken (z.B. postalische Adresse oder E-Mail), ist eine Beantwortung des Antrags (insbesondere Auskunft) grundsätzlich unproblematisch. Trotzdem sollten, insbesondere beim Recht auf Löschung oder Sperrung zusätzliche Informationen des betroffenen (z.B. Kundennummer, Geburtsdatum oder die letzte Rechnungsnummer) abgefragt werden. Immerhin ist es heute nur eine Fingerübung, die Absender-Adresse einer E-Mail zu fälschen.

Antragsteller nicht identisch mit gespeicherten Daten oder Identität nicht zweifelsfrei feststellbar
Erreicht uns ein Antrag beispielsweise telefonisch, sollten grundsätzlich zusätzliche Identifizierungsmerkmale abgefragt werden. In der Regel wird man allein an der Stimme und der gesendeten Telefonnummer niemanden zweifelsfrei identifizieren können. Daher ist es ratsam, die Adressdaten oder die Kundennummer der betroffenen Person abzufragen und mit den gespeicherten Daten abzugleichen. Für besonders sensible Daten dürfte dies jedoch nicht ausreichend sein. Daher ist es sinnvoll, über zusätzliche Verfahren die Identität des Antragstellers zu verifizieren:

1. Kopie des Ausweises

Über die Kopie eines Ausweises kann die Identität des Betroffenen festgestellt werden. Diese Kopie kann per Post oder elektronisch an das Unternehmen zugestellt werden. Zu beachten gilt, dass bei der elektronischen Übermittlung die Sicherheit der Daten im Vordergrund stehen muss. Ist beispielsweise keine Ende-zu-Ende-Verschlüsselung einer E-Mail möglich, sollten Unternehmen einen sicheren Übertragungsweg über ein spezielles Formular mit HTTPS-Verschlüsselung anbieten. Bei der Anfertigung der Ausweiskopie sollte der Betroffene alle nicht für die Identifizierung benötigten Angaben schwärzen.

2. Post-Ident-Verfahren

Über die Deutsche Post kann die Verifizierung einer Person beantragt werden. Dabei wird die betroffene Person durch einen Mitarbeiter der Deutschen Post anhand seines Ausweises identifiziert und die Bestätigung an das Unternehmen verschickt.

3. Double-Opt-In-Verfahren

Es ist auch möglich die Identität einer Antragstellenden Person über ein sog. Double-Opt-In-Verfahren festzustellen. Dabei verschickt das Unternehmen an die gespeicherte Adresse eine E-Mail oder einen Brief mit einem Link oder einem Code, mit Hilfe dessen sich der Betroffene identifiziert.

4. Bearbeitung über ein Kundenkonto

Die einfachste Methode ist die Verifizierung über ein Kundenkonto. Dabei sollte trotzdem stets beachtet werden, z.B. über das Auslesen von Kennwörtern über einen Virus unbefugt Zugriff zum Kundenkonto verschaffen können. Eine Zwei-Faktor-Authentifizierung ist in solchen Fällen ratsam, z.B. über einen Code, der per SMS an die hinterlegte Mobilfunknummer verschickt und bei der Eingabe abgeglichen wird.

Wir helfen gerne!

novinet GmbH & Co. KG
Agentur für digitale Lösungen und Datenschutz

Daniel Steffen
Geschäftsführer novinet
Datenschutzbeauftragter (DSB-TÜV)
Datenschutzauditor (DSA-TÜV)

www.novinet.de
datenschutz@novinet.de
08456 / 3009880

Haftungshinweis

Dieser Artikel wurde auf Basis der aktuell verfügbaren Literatur erstellt. Er dient als erste Einschätzung von potentiellen Problemen innerhalb der Datenschutzgrundverordnung (DSGVO). Es wird darauf hingewiesen, dass viele der hier behandelten Probleme noch nicht abschließend, insbesondere durch höchstrichterliche Rechtsprechungen, geklärt wurden und teilweise auch noch keine Stellungnahmen der Landesdatenschutzbehörden vorliegen, weshalb zu einigen Punkten unterschiedliche Auffassungen vertreten werden. Ich übernehme daher keine Haftung auf Richtigkeit und Vollständigkeit. Insbesondere ist darauf hinzuweisen, dass jeder Fall gesondert zu prüfen ist und dieser Artikel keine Rechtsberatung darstellt.