NUANCE | WHAT'S NEXT BLOG

Kundeninteraktion auf allen Kanälen, Verifizierung und Betrugsprävention

Biometrische Authentifizierung in Zeiten von DS-GVO

Nuance Communications

24 Februar 2020

Die Datenschutz-Grundverordnung (DS-GVO) verunsichert immer noch viele Organisationen, gerade im Hinblick digitaler Transformation und den Einsatz neuer Technologien im Kundenservice. Unternehmen, die sich langfristig vom Wettbewerb abheben möchten, benötigen heute sichere, benutzerfreundliche und schnelle Authentifizierungsmethoden für ihre Kunden. Das aktuelle Whitepaper von Nuance gibt Einblicke in die wesentlichen Richtlinien der DS-GVO und zeigt, welche Möglichkeiten sich für Unternehmen bieten, mit ihr das Vertrauen ihrer Kunden zu stärken.

Ein effizienter und sicherer Kundenservice zählt zu den wichtigsten Eigenschaften langfristig erfolgreicher Unternehmen. Kunden erwarten heute mehr denn je sichere, benutzerfreundliche und schnelle Authentifizierungsmethoden zu ihren Kundendaten. Das führt zwangsläufig zu biometrischen Authentifizierungsmöglichkeiten.

Doch wie können Unternehmen biometrische Lösungen einsetzen und dabei sowohl DS-GVO konform als

auch schnell und effizient agieren? Das Management sensibler Kundendaten ist mit Einführung der DS-GVO höchst komplex geworden, doch nicht unlösbar. Unternehmen müssen selbst dafür Sorge tragen, dass die gesetzlichen Anforderungen erfüllt werden, doch gibt es Funktionalitäten biometrischer Authentifizierungslösungen, die dabei unterstützen. Wie das funktioniert, finden Sie in diesem Whitepaper.

Die Datenschutz-Grundverordnung (DS-GVO)

Die von der Europäischen Union initiierte DS-GVO ist für ihre Mitgliedsstaaten bindend und ersetzt die bis dahin geltenden nationalen Datenschutzgesetze. Diese Verordnung trat im Mai 2018 in Kraft und regelt hauptsächlich die Verarbeitung personenbezogener Daten. Darunter fallen neben allgemeinen Daten (Name, Anschrift, IP-Adresse, etc.) auch biometrische Stimm- und Gesprächsabdrücke. Hinzu kommt das zum gleichen Zeitpunkt eingeführte deutsche Bundesdatenschutzgesetz (BDSG), das insbesondere den geregelten Beschäftigtendatenschutz abdecken soll.

Die Verantwortung für die Einhaltung der datenschutzrechtlichen Anforderungen liegt prinzipiell bei demjenigen, der die Daten erhebt. Ausschlaggebend ist also nicht die technische Lösung an sich, sondern wie der Anwender im datenschutzrechtlichen Sinn mit ihr umgeht. Unternehmen sollten äußerst sensibel bei der Konfiguration entsprechender Systeme vorgehen und zur Absicherung juristischen Rat einholen. Denn die DS-GVO stellt eine Reihe komplexer Anforderungen, dazu zählen unter anderem:

- Rechtmäßigkeit der Datenverarbeitung
- Ausdrückliche Einwilligung der betroffenen Person
- Einhaltung einer umfassenden Informationspflicht
- Abgabe einer detaillierten Datenschutzerklärung
- Zweckbindung und Datenminimierung
- Speicherbegrenzung
- Rechenschaftspflicht

Kurz gesagt, der Gesetzgeber legt Unternehmen bei der Sammlung und Verarbeitung personenbezogener Daten strikte Beschränkungen auf. Diese müssen selbst dafür Sorge tragen, dass sie diesen entsprechen.

Skalierbare und konfigurierbare biometrische Anwendungen unterstützen hierbei. Unternehmen sollten individuell konfigurieren, welche konkreten Daten erhoben, verarbeitet und gespeichert werden. Dies kann abhängig davon erfolgen, wie und zu welchem Zweck die Lösungen eingesetzt werden.

DS-GVO bietet Sicherheit und Chancen

Neben vielen Pflichten bietet die DS-GVO auch Chancen für Organisationen. So ergibt sich die Möglichkeit, das Vertrauen von Kunden zu stärken; beispielsweise, indem sie transparent über den Umgang mit dem sensiblen Datenschutzthema informieren.

Mit biometrischen Lösungen können alle Richtlinien des Gesetzes berücksichtigt werden. Damit erhalten Unternehmen eine gute Ausgangsbasis transparent und regelmäßig mit ihren Kunden zu kommunizieren. Das schafft Vertrauen und verbessert die Kundenbindung entscheidend.

Bevor Sie mit dem Einsatz biometrischer Verfahren zur Kundenauthentifizierung beginnen, stellen Sie sich unter anderem folgende Fragen:

- Welche Daten wollen Sie wie lange und zu welchem Zwecke erheben und speichern?
- Wer darf und soll auf diese Daten zu welchem Zwecke zugreifen?
- Wie informieren Sie Ihre Kunden und Mitarbeiter über die Sammlung, Verarbeitung und Speicherung personenbezogener Daten?
- Wie stellen Sie sicher, dass Ihre Kunden und Mitarbeiter zu jeder Zeit Zugriff auf die von Ihnen gesammelten Daten haben und diese löschen lassen können?
- Welchen Mechanismus halten Sie vor, um die Sicherheit der personenbezogenen Daten in Ihrem Unternehmen zu gewährleisten?
- Kennen Sie und die mit der Verarbeitung personenbezogener Daten betrauten Mitarbeiter die Datenschutz-Folgeabschätzung Ihres Unternehmens?

Tags: Sprachbiometrie, Spracherkennung, Sprachtechnologie, Biometrische Authentifizierung