Authentifizierung: Anruf im Call-Center – Wie wissen die Mitarbeiter*Innen des Verantwortlichen, dass sie mit der richtigen Person sprechen?

Fehler können zu DSGVO-Strafen führen.

Warum ist das relevant?

Bei 1&1 Deutschland kam es wegen **mangelhafter Authentifizierung** eines Anrufers zu einer **Weitergabe von personenbezogenen Daten an jemanden, der sich für einen Kunden ausgegeben** hat. Dies führt zu einem **Bußgeld** in erster Instanz von **EUR 9,5 Mio** und in der zweiten Instanz wurde die **DSGVO-Geldstrafe auf EUR 900.000,-- vom Landgericht Bonn reduziert**.

Das Urteil liegt nun im Volltext vor, und darauf sind nicht nur im Hinblick auf die Strafhöhe Schlüsse zu ziehen.

Fest steht: eine **mangelhafte (oder gar fehlende) Richtlinie zur Authentifzierung** von **Anrufern**, die dann dazu führen kann, dass **unbefugte Personen Informationen** (personenbezogene Daten) erhalten, kann zu einer **erheblichen DSGVO-Strafe führen**.

Aus **Krankenhäusern** oder bei **Service-Hotlines von Mobil-Service/Internetprovidern** kennen wir es mittlerweile, die Frage:

Könnten Sie uns bitte das persönliche Kennwort / Passwort sagen?

Diese Rückfrage dient der **Sicherheit**, dass diejenige Person, die gerade anruft, zumindest das Passwort / Kennwort weiß, und daher berechtigt ist, Informationen zu erhalten. Diese „Routine“ solle jedenfalls in eine schriftliche Dienstanweisung einfließen, damit gegenüber etwaigen Datenschutzaufsichtsbehörden (im Sinne der

Accountability oder **Rechenschaftspflicht**) nachgewiesen werden kann, dass es eine derartige **Richtlinie gibt**, und dass **die zuständigen Mitarbeiter*Innen** auch in der Handhabung derartiger Anrufe **geschult** sind, und sich daran halten.

Der Sachverhalt in der Entscheidung des LG Bonn

Authentifzierung von anrufenden Personen beim Verantwortlichen

In der Entscheidung des LG Bonn wird dies so geschildert (Hervorhebungen und Absätze vom Autor):

„b) **Anrufer** erreichten im Callcenter in der Regel als erstes einen Serviceagenten des **First-Level-Supports**. Dieser musste den Anrufer zunächst **identifizieren**.

Erfolgte der Anruf unter einer **von K vergebenen Telefonnummer** wurde dem Serviceagenten der jeweilige Datensatz der **Telefonnummer direkt** angezeigt.

Handelte es sich dagegen um einen **Anruf von einer fremden oder unterdrückten Telefonnummer** wurde der Kunde vom Serviceagenten anhand seines **Namens** und seines **Geburtsdatums** oder – alternativ – durch **Angabe von Kunden-/Vertrags- bzw. Auftragsnummer identifiziert**.

22 Der jeweilige Serviceagent war angehalten, den Anrufenden als Berechtigten zu authentifizieren. Hierzu wurde – soweit dies nicht bereits für den Aufruf des richtigen Datensatzes im Rahmen der Identifizierung erforderlich war – das **Geburtsdatum** abgefragt.

23 **Nach der Authentifizierung** waren die Callcenter-Agenten ermächtigt, dem Anrufer **Auskünfte zu erteilen** und **Änderungswünsche** entgegenzunehmen.

Bei bestimmten Themen leiteten die Callcenter-Agenten des First-Level-Support auf der **Grundlage eines Berechtigungskonzepts** die Anrufer an **andere Mitarbeiter weiter**. So konnte etwa nur die Rechnungsstelle eine neue **Bankverbindung** eingeben. **Eine nochmalige oder strengere Authentifizierung erfolgte gegenüber** diesen weiteren Mitarbeitern nach der Authentifizierung durch den First-Level-Support **nicht**.

24 Für den Fall, dass für den **Callcenter-Agenten erkennbar eine andere Person** als der Kunde im Callcenter **anrief**, hatte die Betroffene **keine umfassende Regelung** getroffenen.

Lediglich für den Umgang mit **telefonischen Anfragen von gesetzlichen Betreuern** gab es eine besondere **Arbeitsanweisung**.

Im Übrigen entsprach es bei der Betroffenen **gängiger Praxis**, dass **Personen, die sich als Familienangehörige des Kunden oder sonst nahestehende Personen** vorstellten und zur **Authentifizierung den Namen und das Geburtsdatum des Kunden** nennen konnten, als **legitimiert** galten, **für den Kunden zu handeln**. Dies war unabhängig davon, ob **diese Person vom Kunden** als sog. **weiterer Ansprechpartner** im System hinterlegt worden war oder nicht.

Nicht ausdrücklich **geregelt** war auch, wie die Callcenter-Agenten reagieren sollten, wenn ein **anrufender Dritter im Rahmen** des Authentifizierungsprozesses das **Geburtsdatum** des Kunden **nicht nennen konnte**.

25 Die Authentifizierung der Anrufer im Callcenter wurde bei der Betroffenen schon seit mehreren Jahren **wie vorstehend beschrieben praktiziert**. Eine **Überprüfung** dieser **Praxis auf ihre Konformität mit der Datenschutzgrundverordnung erfolgte nicht**."

Der Sachverhalt, der zum „Aufdecken" dieses Systems der Authentifizierung führte

Die Ex-Lebensgefährtin eines Kunden nutzte dieses System aus. Der Kunde hatte die Telefonnummer bewußt geändert, damit die Ex-Lebensgefährtin ihn nicht mehr anrief.

Der Ex-Lebensgefährtin des Kunden war offensichtlich bekannt, dass es zu einer Sperre beim Kunden gekommen war und sie rief am 23.12.2018 beim Call-Center des Verantwortlichen an, „**gab sich als Ehefrau des Kunden** aus und erklärte, dass sie die **offene Forderung beglichen** habe. Da sie den **Namen** und das **Geburtsdatum** ihres **Ex-Partners** nennen konnte, wurde sie durch die C**allcenter-Agentin als Berechtigte behandelt**. Im Zuge des Gesprächs wurde der Anruferin die **neue Telefonnummer ihres Ex-Partners bekannt gegeben**."

Die **neue Telefonnummer**, die sie auf diesem Weg erfahren hat, nutze sie und belästigte ihren Ex-Lebensgefährten, dh den Kunden des Verantwortlichen. Dieser erstattete Anzeige bei der Polizei wegen **Stalkings**.

Die zuständige Aufsichtsbehörde erfuhr durch eine Mitteilung durch die Polizei vom 31.1.2019 vom Vorgang und leitete ein **Ermittlungsverfahren** wegen Verstoßes gegen die DSGVO, nämlich **mangelhafter technischer und organisatorischer Maßnahmen iSd Art 32 DSGVO** ein.

Andere (Mobilfunk)-Unternehmen identifizieren ihre **Kunden** bzw. die **Anrufer im Call-Center** mit folgenden **Routinen**:

- Tochter ruft ausdrücklich für ihre Mutter an und nennt deren Kundennummer, Namen und Geburtsdatum. Eine Vollmacht wird nicht verlangt.
- Der Anrufer authentifiziert sich über die im Vertrag hinterlegte Mobilnummer unter Angabe von Geburtsdatum und Anschrift.
- Der Anrufer authentifiziert sich mit Kundennummer, Namen, Geburtsdatum.
- Der Anrufer muss die OCard-Nummer angeben.
- Anrufer wird nach seiner 4-stelligen PIN gefragt. Falls diese nicht zur Hand ist, wird eine Authentifikations-TAN auf das Endgerät geschickt.
- Falls ein Anrufer seine Vertragskontonummer nicht zur Hand hat, genügt die Angabe von Nachname, Postleitzahl und Geburtsdatum.
- Es genügt die Angabe von KFZ-Kennzeichen, Name und Geburtsdatum.
- Falls ein Anrufer seine Vertragsnummer oder Kundennummer nicht zur Hand hat, genügt die Angabe des Namens und des Geburtsdatums des Vertragsinhabers.
- Es wird die Kundennummer, Name, Anschrift und Geburtsdatum abgefragt.
- Es genügt die Kundennummer, falls nicht zur Hand reichen auch Name und Geburtsdatum.

Nach Einleitung des Ermittlungsverfahrens hat der Verantwortliche eine „Notmaßnahme“ zur Authentifizierungsroutine gesetzt. Es wurden folgende **Daten zur Authentifizierung** abgefragt:

- die **Kunden-/Vertrags- oder** Auftragsnummer,
- das **Geburtsdatum** bzw. die **Emailadresse** und
- die **letzten vier Ziffern der IBAN**

Es war eine Systemumstellung notwendig, um eine höherwertige Identifizierungsroutine im Unternehmen einzuführen. Dieses System startete Ende 2019, und nun erfolgt die **Identifizierung** im Call-Center mittels einer **fünfstelligen Service-PIN**, die dem Kunden per Post / per E-Mail zugesendet wurde, und die auf eine „**Wunsch-PIN**“ geändert werden kann.:

„kleine Ursache“ – „große Wirkung“

Die **mangelhafte Identifizierungsroutine**, die es ermöglichte, relativ leicht – nämlich durch Angabe des Namens und des Geburtsdatums - zur an **wenig kritischen Information** (Telefonnummer des Kunden) zu kommen, führte letztlich zu einem **Bußgeld** in Höhe von **EUR 9,5 Mio** in der ersten Instanz, und **EUR 900.000,--** in der zweiten Instanz sowie zu **Umstellungskosten in Höhe von mehreren Millionen EURO.**

Was ist zu tun – Call-Center-Authentifizierungsroutinen

Es ist wesentlich, dass sich jedes Unternehmen, das **Informationen** über natürliche Personen am „**Telefon**“ **herausgibt**, diese Informationen, auch wenn diese per se keinen besonders eingriffsintensiven Charakter oder augenscheinlich gar nicht „so privat“ sind, wie es zB die Kontoverbindung oder Verbindlichkeiten beim Unternehmen oder Art 9 / Art 10 Daten sind, auch missbräuchlich verwendet werden könnten.

Die Authentifizierung beim Anruf hat daher sicherzustellen, dass **die Call-Center-Mitarbeiter*Innen** mit der „**richtigen**“, dh einer **befugten Person sprechen**, und die Informationen auch an diese Person herausgeben dürfen.

Die Identifizierung mit **Namen**, **Adresse** und **Geburtsdatum** allein reicht keinesfalls aus.

Die Vergabe eines **PIN** oder eines **Passwortes / Kennwortes**, das in der **Call-Center-Software hinterlegt wird**, und beim **Anruf abgefragt** wird, ist eine der Möglichkeiten, die genutzt werden können.

Ein Verantwortlicher, der telefonisch Auskünfte erteilt, die auch nur indirekt personenbezogene Daten von natürlichen Personen enthalten, hat durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass diese Daten nicht an unberechtigte Personen herausgegeben werden.

Sinnvollerweise sollte daher jedes Unternehmen mit einer Support-Hotline eine entsprechende, auch

1. dem Risikoniveau angemessene **Richtlinie zur Authentifizierung von Anrufern und berechtigen Personen** erstellen,

2. die **Mitarbeiter*Innen in** der Handhabung der Richtlinie **schulen** und
3. auch gelegentlich durch **Testanrufe** die Einhaltung prüfen bzw. sicherstellen.

Dabei ist zu bedenken, dass selbst **einfache Datensätze** wie **Telefonnummer** oder **Adresse** oder auch nur die Tatsache, dass eine Person in einem **Vertragsverhältnis** zum Verantwortlichen steht, nicht ohne weiteres bekannt geben werden sollten, da der **Übermittlungsempfänger** uU eine **besondere Beziehung** zur betroffenen Person hat, und diese **Informationen zum Nachteil derselben verwenden könnte**.

Wenn die Aufsichtsbehörde feststellt, dass die Authentifizierungsroutine oder die gelebte Praxis nicht ausreichend ist/war, um die personenbezogenen Daten der Kunden oder anderer natürlicher Personen zu schützen, dann kann es zu einem empfindlichen Bußgeld kommen. Die DSGVO-Strafe trägt der Verantwortliche, der sich nicht ausreichend darum gekümmert hat, technische und organisatorische Maßnehmen zu implementieren, die eine derartige Offenlegung an unberechtigte Personen (Datenschutzverletzungen; data leaks) verhindern.

Ein **Regress**, bei der Person, die vorsätzlich und mißbräuchlich das System des Verantwortlichen ausgenützt hat, erscheint mir nicht möglich, da die **Feststellung des DSGVO-widrigen Verhaltens** zwar uU wegen der mißbräuchlichen Verwendung der Aufsichtsbehörde bekannt wird, aber das Verschulden an der mangelhaften Einhaltung des Art 32 DSGVO nicht in einem direkten Zusammenhang mit dem konkreten data-leak steht, sondern ein Organisationsverschulden darstellt, das nur durch diese Tatsache aufgedeckt wurde.