Klantverificatie in contactcenters: klantvriendelijk of niet

Category: Groeimodel en Processen
written by SteinBlogs | 21 December 2025

Kernpunten

- **Klantverificatie** controleert of contactpersonen echt zijn wie ze zeggen te zijn—cruciaal voor privacy en fraudepreventie
- **36% van consumenten** heeft fraudepogingen met klantgegevens meegemaakt; bij jongeren (18-34) is dit 52%
- **Verificatie is klantvriendelijk** als je uitlegt waarom het nodig is—ergernis daalt van 70% naar 40%
- **Basisgegevens** zoals naam, geboortedatum en postcode volstaan meestal; bij financiële zaken zijn extra stappen nodig
- **Multifactor authenticatie (2FA/MFA)** bespaart tot 45 seconden per contact en maakt verificatie 50% sneller
- **Goede communicatie** is essentieel: leg vooraf uit welke gegevens nodig zijn en waarom dit in het belang van de klant is

Inhoud

- Kernpunten
- Wat is klantverificatie en waarom is het belangrijk?
  - Wat is het verschil tussen identificatie en verificatie?
- Waarom is klantverificatie belangrijk?
  - 1. Toegankelijkheid betekent niet altijd voorbereiding
  - 2. Identiteitsmisbruik en fraude
  - 3. Ook fraudeurs profiteren van nieuwe technologie
  - 4. Wetgeving verlangt zorgvuldigheid
- Is klantverificatie klantvriendelijk of bureaucratisch?
- Welke gegevens mag je redelijkerwijs vragen?
  - Basisgegevens bij bestaande klanten:
  - Extra verificatie bij grotere verzoeken:
  - Wat een bedrijf nooit mag vragen:
- Hoe verloopt klantverificatie in de praktijk?
  - Situatie 1: Een onbekend contractnummer
  - Situatie 2: De IBAN-check bij een nieuwe verzekering
- Hoe maak je klantverificatie efficiënter?
  - 1. Informeer klanten vooraf
  - 2. Leg kort en vriendelijk uit waarom
  - 3. Wees duidelijk over wat je nooit vraagt

    - 4. Geef een oplossing
    - 5. Uniforme en efficiënte werkwijze
    - 6. Bied alleen processen aan die passen bij het verzoek
    - 7. Overweeg face-to-face verificatie voor complexe zaken
- Welke verificatiemethoden werken het beste?
- Wat is de belangrijkste les over klantverificatie?
- Veelgestelde vragen over klantverificatie (FAQ)
    - Hoe verloopt het verificatieproces in de praktijk?
    - Welke gegevens vraagt een bedrijf tijdens verificatie?
    - Kan ik klantverificatie automatiseren in mijn contactcenter?
    - Wat zijn de beschikbare methoden om klanten te verifiëren?
    - Hoe help ik klanten die geen gegevens bij de hand hebben?
    - Moeten we voor elk verzoek dezelfde voorschriften hanteren?
    - Wat moet ik doen als klanten verificatie frustrerend vinden?
    - Kunnen we verificatie volledig digitaal laten verlopen?
    - Hoe verstrekken klanten veilig klantgegevens tijdens verificatie?
    - Waar kunnen we ons verificatieproces verbeteren?
- Verder lezen?
- English Summary
- Resumen en Español

Wat is klantverificatie en waarom is het belangrijk?

Klantverificatie controleert of iemand die contact opneemt echt is wie hij zegt te zijn, voordat gevoelige gegevens worden gedeeld of wijzigingen doorgevoerd.

We leven in een wereld waarin we met één swipe kunnen bestellen, met één klik kunnen annuleren en met één ingesproken voicebericht kunnen klagen. Ik doe het zelf ook. Tussen twee afspraken door bellen we even de energiemaatschappij bellen vanuit de trein. Of sturen een chatbericht naar de ziektenkostenverzekeraar. We laten via sociale media weten dat “nu” iets moet worden opgelost.

Maar in die vanzelfsprekendheid schuilt iets merkwaardigs. Stel: ik bel onvoorbereid een bedrijf om mijn contract wijzigen. Waarom verwacht ik dan dat zij wél alle gegevens paraat hebben? En belangrijker: hoe weten zij eigenlijk dat ik echt ben wie ik zeg dat ik ben?

Voor contactcenters en klantenservice medewerkers is dit geen filosofische exercitie maar dagelijkse werkelijkheid. Zij moeten de balans vinden. We willen allemaal klantgemak en we verwachten allemaal zorgvuldigheid. Voor een medewerker moet eerst helder zijn met wie hij spreekt. Daarna mag hij pas iets aanpassen, wijzigen of inzien. Niet om de klant te pesten. Nee, om te beschermen.

Wat is het verschil tussen identificatie en verificatie?

Klantidentificatie: de persoon identificeren waarmee je een zakelijke relatie aangaat. Klantverificatie: vaststellen of de persoon die belt, chat of mailt ook echt de klant is.

Laten we even scherp krijgen over de begrippen die we gebruiken. We schrijven **klanten.** Dat zijn dus consumenten, burgers, patiënten, cursisten of zakenrelaties enzovoorts. Met **verzoeken** bedoelen we producten en diensten. Dit varieert van bestellingen, boekingen en reserveringen, contractwijzigingen, informatievragen tot garantieclaims en meer. En wij noemen **bedrijven**, maar dat zijn ook gewoon winkels, instanties of organisaties.

We onderscheiden drie begrippen (en dat is geen semantische trukendoos, maar belangrijk):

- **Klantidentificatie**: een persoon identificeren waarmee je een zakelijke relatie aangaat. Bijvoorbeeld om een account aan te maken.
- **Klantverificatie**: vaststellen of de persoon die belt, chat of mailt ook echt de klant is.
- **Verificatie van klantgegevens**: controleren of gegevens bestaan en een juist formaat hebben. Is dit een geldig e-mailadres, bestaat deze postcode echt?

Dit artikel gaat over Klantverificatie. Hoe verifieer je dat de stem aan de lijn, of het getypte bericht in de chat of mail horen bij de persoon die ze zeggen te zijn?

Waarom is klantverificatie belangrijk?

Klantverificatie voorkomt identiteitsfraude, beschermt privacy, voldoet aan AVG-wetgeving en waarborgt dat alleen bevoegden wijzigingen doorvoeren.

De drempel om contact op te nemen is lager dan ooit. Telefoon, e-mail, chat, app, website, sociale media: een vraag is zo gesteld. Paradoxaal genoeg vergroot dat digitale gemak juist de kans op misverstanden, fouten én misbruik.

Uit Engels onderzoek (2023) onder klanten van contactcenters zegt 36% van consumenten fraudepogingen met hun klantgegevens te hebben meegemaakt. Onder jonge consumenten (18-34 jaar) ligt dit met 52% veel hoger, mogelijk omdat zij vaker (ongemerkt) persoonlijke gegevens online op social media delen.

Er zijn vier redenen waarom klantverificatie dan belangrijk is:

1. Toegankelijkheid betekent niet altijd voorbereiding

Omdat iedereen elk moment kan bellen of appen, bereidt de klant zich minder voor. Hij heeft zijn gegevens niet altijd bij de hand. Dat klinkt logisch misschien. Het risico dat iemand anders namens hem belt neemt daardoor toe. Of dat nu goedbedoeld is (een partner) of kwaadwillend (een fraudeur).

2. Identiteitsmisbruik en fraude

Als iemand zich als jou voordoet, kan hij je gegevens verkrijgen, je contract veranderen of namens jou een bestelling doen. De gevolgen? Inbreuk op je privacy en veiligheid. Je lijdt reputatieschade of krijgt financiële ellende.

3. Ook fraudeurs profiteren van nieuwe technologie

Ons leven wordt makkelijker met nieuwe techniek. Helaas geldt dat ook voor fraude. Één goede hack en duizenden klantgegevens liggen op straat. De techniek die fraudeurs gebruiken wordt steeds geraffineerder. Databescherming moet dus mee-evolueren.

4. Wetgeving verlangt zorgvuldigheid

Organisaties moeten zorgvuldig zijn met persoonsgegevens. Dat regelt privacywetgeving zoals AVG. Die wettelijke eisen zijn prima maar in de basis is het simpel: ik wil dat mijn data veilig is. Jij waarschijnlijk ook.

De vraag blijft dus: hoe weet je zeker dat de persoon die belt écht is wie hij zegt te zijn?

Is klantverificatie klantvriendelijk of bureaucratisch?

Klantverificatie is klantvriendelijk omdat de klant beschermt tegen fraude, net zoals een paspoortcheck bij vliegtuigen normaal is.

Het is té gemakkelijk om verificatie bureaucratisch gedoe of klantonvriendelijk te noemen. Op LinkedIn reageren klantcontact-experts verontwaardigd als bedrijven vragen naar zoiets als een contractnummer. Zo’n bericht doet het natuurlijk goed. Maar is dat wel terecht?

Denk eens aan situaties die we volkomen normaal vinden:

- Bij het boeken van een vlucht weten we dat ons paspoort nodig is
- Een artikel ruilen? Kassabon graag
- Inloggen bij de Belastingdienst? DigiD natuurlijk
- Online betalen? Verificatie via de bankapp

Is het dan vreemd dat een bedrijf je een polisnummer vraagt als je zelf belt over je verzekering? Of je energieleverancier je contractnummer? En de laatste cijfers van je IBAN als je iets wilt wijzigen met financiële gevolgen?

Het is een tweerichtingsverkeer. Als ik als klant een verzoek doe, mag het bedrijf verwachten dat ik me enigszins voorbereid. Niet omdat ze lastig willen zijn, maar omdat ze in mijn belang willen handelen. Als klant verwacht ik dat ze zorgvuldig zijn met mijn gegevens. Zonder die juiste gegevens kunnen ze simpelweg niet zorgvuldig zijn. Of ze dat nu wettelijk verplicht of niet.

Dus als een medewerker vraagt “Heeft u uw klantnummer bij de hand?”, is dat dan werkelijk onredelijk? Het is toch logisch dat ik, wanneer ik bel over mijn contract, zélf weet over welk contract het gaat? Ik kan het natuurlijk proberen zonder voorbereiding. Prima als dat goed gaat. Waarom moeilijk doen als het makkelijk kan? Als het niet lukt: neem zelf verantwoordelijkheid. De medewerker is dan *juist* klantvriendelijk.

Maar wat in dit artikel een rol speelt, is vooral ‘friction reduction’. De klant vindt het vreemd dat wij hem niet kennen, hij is immers toch klant? En als we dan om persoonlijke gegevens vragen, maakt dit het eerder erger dan beter. Het kan een riedeltje zijn dat een agent steeds weer afraffelt omdat bij iedere call opnieuw moet. En dat we daarom geen moeite nemen en klantverificatie toepassen zonder de context te benoemen. In die gevallen, vindt 70% van de klanten al die vragen frustrerend bij onduidelijke communicatie. Ja, dan is het bureaucratisch en inderdaad klantonvriendelijk. Geen excuus.

Licht de medewerker de context van klantverificatie beter toe, dan neemt de ergernis al snel af van 70% tot minder dan 40%. Er ontstaat meer begrip bij de klant. En belangrijk: het geeft vertrouwen als je toelicht dat het ook om klantbelang gaat.
Iets dat we vaak negeren, simpelweg omdat wij het zelf niet aan den lijve ondervinden is het volgende. In de optiek van de klant blijft de totale optelsom van alle tijd voordat hij überhaupt zijn vraag kan stellen en een antwoord krijgt, vaak frusterend lang: dus de wachttijd, tijd in de IVR, luisterend naar meldteksten gevolgd door controlevragen van medewerkers, plus de reële mogelijkheid dat de klant zijn verhaal nog ‘ns moet herhalen. En dan blijft de ergernis en bereik je hooguit een sub-optimum.

Welke gegevens mag je redelijkerwijs vragen?

Bedrijven vragen meestal naam, geboortedatum, postcode, huisnummer en een klantnummer. Bij financiële zaken komen er de laatste cijfers van een IBAN rekening of security codes bij.

Niet alles hoeft meteen zwaar beveiligd te worden. Controles hoeven niet bureaucratisch te zijn. De basis ligt bij proportionaliteit. Een bedrijf moet

weten wie de persoon is die vraagt om een account, boeking of contract te veranderen. Dat bepaalt welke gegevens nodig zijn.

Basisgegevens bij bestaande klanten:

Gevraagde gegevens bestaan meestal uit een combinatie van het volgende:

- Naam en voorletters
- Geboortedatum
- Postcode en huisnummer
- E-mailadres
- Een nummer (contract-, klant-, polis-, boeking- of reserveringsnummer)

Dit is meestal laagdrempelig. Ze dienen vooral om snel het CRM-systeem te doorlopen en aan een eerste check te voldoen. Steeds vaker vragen medewerkers naar recent contact of iets anders dat alleen de klant kent.

Extra verificatie bij grotere verzoeken:

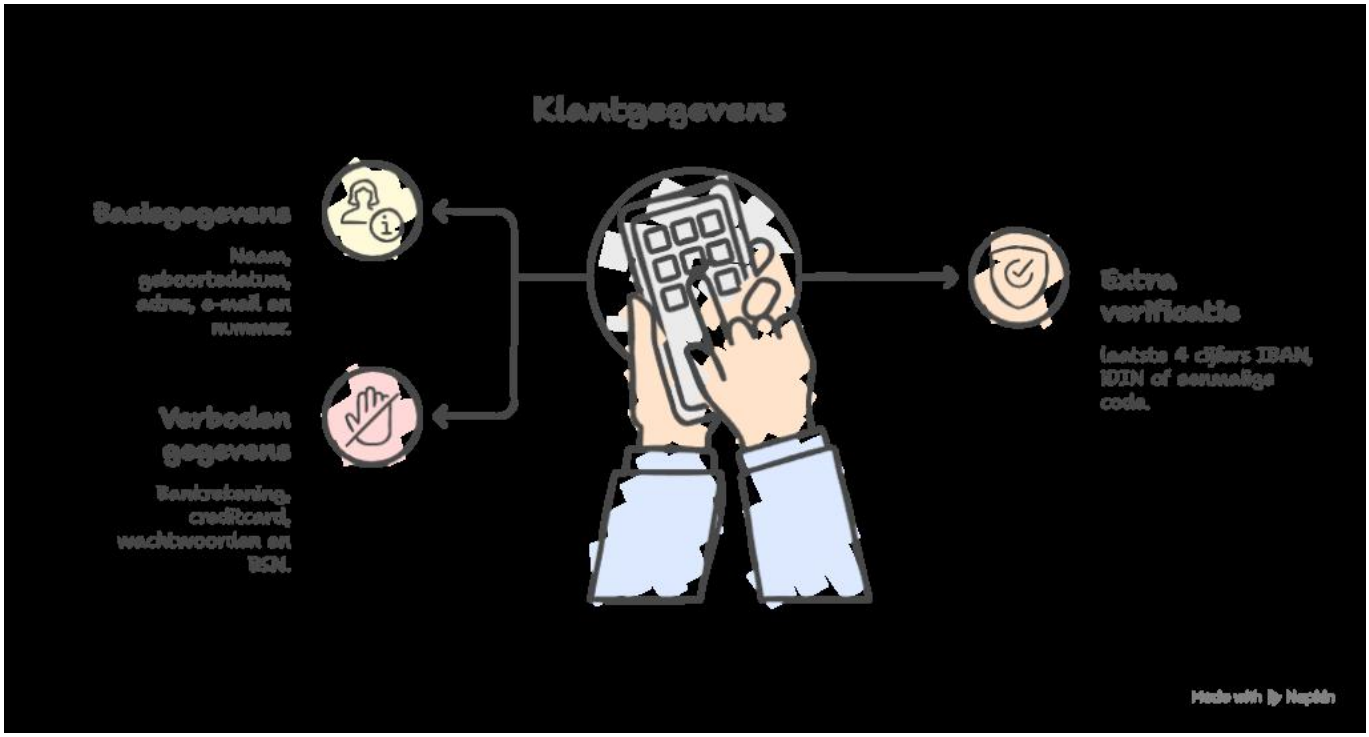
Bij financiële consequenties of ingrijpende wijzigingen kan een extra stap worden gevraagd:

- De laatste cijfers van een bekend IBAN
- Verificatie via internetbankieren (iDIN)
- Een eenmalige code verzonden per app, e-mail of sms

Bij bellen helpt herkenning van het telefoonnummer op de achtergrond mee. Komt het overeen met het geregistreerde nummer? Niet? Dat bepaalt of een medewerker extra vragen stelt. Of vraagt hij aan de klant om terug te bellen vanaf het nummer dat bekend is.

Wat een bedrijf nooit mag vragen:

- Volledige bankrekeningnummers
- Volledige creditcardgegevens
- Wachtwoorden of login gegevens
- Het BSN-nummer (behalve bij wettelijk verplichte overheidsprocessen via DigiD)



Hoe verloopt klantverificatie in de praktijk?

Het verificatieproces verloopt meestal in stappen waarbij eerst basisgegevens worden gevraagd, gevolgd door aanvullende controles afhankelijk van het verzoek.

De spanning ontstaat precies daar waar klantgemak botst met zorgvuldigheid. Twee voorbeelden.

Situatie 1: Een onbekend contractnummer

Een man belt een energiemaatschappij. Hij hoorde iets op de radio over een goedkoper tarief. Hij vraagt of die prijs ook voor zijn huidige contract kan. Ja, zegt de medewerker, dat kan. Mooi, zegt de klant, regel dat dan maar meteen. Maar dan: “Heeft u uw contractnummer bij de hand?” Nee, dat heeft hij niet. En hij vindt het maar onzin dat dit wordt gevraagd. De medewerker mag niet verder. Onbegrip bij de klant en ongemakkelijk voor de agent. En dat terwijl het proces eigenlijk in het belang van de klant is en op zijn initiatief ontstaat.

Situatie 2: De IBAN-check bij een nieuwe verzekering

Een vrouw wil telefonisch een verzekering afsluiten. Dat kan, zegt de medewerker. U ontvangt een betaalverzoek (vaak €0,01) via Ideal of met een Tikkie. Hiermee bevestigt u uw identiteit en rekeningnummer voor premiebetaling. Maar de vrouw belt uit de auto en kan dat nu niet doen. Het proces moet worden gepauzeerd. Voor haar voelt dat als vertraging. Voor de medewerker is het de correcte werkwijze.

Beide voorbeelden laten zien: het draait om verwachtingsmanagement. Leg kort

uit waarom zulke stappen nodig zijn. Toon begrip en bied aan om het gepauzeerde verzoek een unieke code te geven. Hiermee kan de klant later kan terugbellen zonder alles opnieuw te herhalen.

Hoe maak je klantverificatie efficiënter?

Informeer klanten vooraf welke gegevens nodig zijn, leg kort het waarom uit, en bied alternatieven zoals portals of terugbellen aan.

1. Informeer klanten vooraf

Vertel duidelijk welke gegevens iemand bij de hand moet hebben op je website, in je portal, in e-mails en in telefonische meldingen . Bijvoorbeeld:

> *“Belt u over uw verzekering? Houd dan uw polisnummer bij de hand.”*

Je kunt eraan refereren. Dit voorkomt frustratie. Het maakt het proces makkelijker voor beide partijen.

2. Leg kort en vriendelijk uit waarom

Een simpele zin helpt al:

> *“Ik vraag u dit om zeker te weten dat ik de juiste persoon spreek en het beschermt uw belangen.”*

Mensen begrijpen het als je de voordelen benoemt. Het gebeurt in hun eigen belang.



3. Wees duidelijk over wat je nooit vraagt

Veel klanten voelen zich veiliger als een bedrijf dit steeds opnieuw benoemt:

- Nooit het volledige banknummer
- Nooit wachtwoorden
- Nooit het volledige creditcardnummer

Dit geeft vertrouwen.

4. Geef een oplossing

Zonder de juiste gegevens kun je voor de klant niet verder. Wees hierover begripvol en duidelijk. En biedt oplossingen aan zoals:

- Bewaar het verzoek voor de klant en sla het op met een unieke code.
- Vraag of de klant later met de code terugbelt.
- Vertel dat het 24/7 mogelijk is om het verzoek in de portal te doen.

Dit voorkomt ergernis. Je creëert begrip en laat zien dat je meedenkt.

5. Uniforme en efficiënte werkwijze

Vergelijkbare verzoeken volgen dezelfde stappen ongeacht het contactkanaal. Medewerkers vragen dezelfde gegevens via telefoon, chat, e-mail of sociale media. Dat betekent: goede templates, kennisbankartikelen in je CRM, en checklists die helder zijn.

Een slimme methode: de medewerker doet (traceerbaar) voor de klant het verzoek in de portal. Je doorloopt dezelfde stappen die de klant anders zelf zou moeten doen. Let op: verificatie die de klant normaal doet, moet hij nog steeds zelf doen! Als de portal automatisch een SMS code stuurt, moet de klant die kunnen bevestigen.

Klantverificatie in live contact bespaart met 2FA of MFA tot gemiddeld 45 seconden per contact. We zien voorbeelden dat contactcenters die multifactorauthenticatie (2FA of MFA) gebruiken, de verificatie 50% sneller kunnen afronden. Uiteraard moet de inzet van het middel het doel rechtvaardigen zoals bij klantverzoeken met financiële consequenties of gevolgen die ingrijpen in de persoonlijke levenssfeer.

Als die technologie aanwezig is, gebruik die dan. Het voorkomt dubbele processen en training. De medewerker leert de (on)mogelijkheden van de portal kennen zoals ook een klant die ervaart. Je maakt de klant wegwijs in de portal zodat hij het later zelf kan. En werkt zo gericht aan de digitale toekomst.

6. Bied alleen processen aan die passen bij het verzoek

Probeer vooral niet om alle verzoeken via elk kanaal te honoreren. Dat is niet realistisch en garantie voor falen. Grote wijzigingen horen soms gewoon thuis in het klantportaal of zelfs live bij een fysieke locatie. In een correct beveiligde digitale omgeving is meteen helder dat het werkelijk de klant is die iets vraagt.

Denk aan:

- Online zelf een verhuizing doorgeven
- Contractwijzigingen via het portal
- Bestellingen die automatisch geverifieerd worden via betaling

Voor speciale gevallen blijft persoonlijk contact mogelijk. Benoem die situaties met heldere kaders.

7. Overweeg face-to-face verificatie voor complexe zaken

Sommige dingen vragen nu eenmaal persoonlijke aanwezigheid. Denk aan het aanvragen van een paspoort of rijbewijs. Vaak staat dat proces dankzij DigiD al grotendeels online. Op een gegeven moment moet je als klant toch fysiek naar een balie. En dat is prima. Toch verandert ook dit razendsnel. Bijvoorbeeld banken die persoonlijk contact vervangen met een virtuele

variant. Ze vragen je als klant om (meerdere) selfies náást een kopie identiteitsbewijs.

Een bedrijf moet bewust kiezen: welke manier van controleren past bij welk verzoek? Welke risico's zijn echt belangrijk in de praktijk? Zonder bureaucratische regels te maken die klanten alleen maar lastig vallen. En controleren of de regels goed werken, juist bij technologie die alsmaar verandert.

Welke verificatiemethoden werken het beste?

Verificatiemethode	Snelheid	Veiligheid	Beste gebruik voor
Login portal/app	Zeer snel	Zeer hoog	Routine-verzoeken, zelfservice
2FA/MFA (code per sms/email/app)	Snel (45 sec. besparing)	Hoog	Financiële transacties, contractwijzigingen
Telefonische verificatie (kennisvragen)	Gemiddeld	Gemiddeld	Algemene vragen, eerste contact
iDIN (internetbankieren)	Snel	Zeer hoog	Identiteitsverificatie, nieuwe contracten
DigiD	Snel	Zeer hoog	Overheidsprocessen, BSN-gerelateerd
Terugbellen naar geregistreerd nummer	Traag	Gemiddeld	Ongebruikelijke verzoeken, extra check
Face-to-face/fysieke locatie	Zeer traag	Zeer hoog	Identiteitsdocumenten, complexe zaken
Biometrische verificatie (stem/iris/vingerafdruk)	Zeer snel	Zeer hoog	Hoogwaardige beveiliging (beperkt in NL)

MFA (Multifactor authentication) en 2FA (two-factor authentication) zijn in opkomst bij live klantcontact. Nog steeds moet de klant een of enkele typische kennisvragen beantwoorden die alleen hij zou weten. Dit wordt nu echter technisch aangevuld met bevestiging van een code die de klant ontvangt via geregistreerde e-mail, app of authenticator. Zonder bevestiging van de juiste code, kan het aan het klantcontact gekoppelde verzoek (een transactie, al dan niet financieel) niet worden uitgevoerd. Dit lijkt 99,99% waterproof. De zwakte zal ook hier zijn dat zulke hoge betrouwbaarheid altijd zal worden ondermijnd indien de toegang tot persoonsgegevens bij bedrijven en instanties onvoldoende is gewaarborgd. In augustus 2025 bleek bijvoorbeeld dat bijzonder veel persoonlijke gegevens waren buitgemaakt bij een hack bij het bureau (laboratorium) dat de uitslagen van bevolkingsonderzoeken beheert. Aanvulling met biometrische gegevens (stemprofiel, irisscan, vingerafdruk etc.) is een mogelijkheid om de veiligheid verder te verhogen maar stuit in een land als Nederland als snel op bezwaren omtrent privacy.

Wat is de belangrijkste les over klantverificatie?

Klantverificatie ís klantvriendelijk, mits je uitlegt waarom. Het draait om verwachtingsmanagement en balans tussen gemak en zorgvuldigheid.

Het draait om verwachtingsmanagement. Medewerkers kunnen vriendelijk en duidelijk uitleggen dat ze gegevens juist vragen vanuit klantbelang. Vaak valt dan al veel weerstand weg. En als een klant niet voorbereid is? Geen probleem. Bied alternatieven, geef geruststelling, laat zien hoe het wél kan.

Het draait om balans. De balans tussen gemak en zorgvuldigheid. Tussen snelheid en veiligheid. Tussen “nu meteen regelen” en “even de juiste gegevens bij de hand”.

Als je gegevens vraagt, wees dan helder over de reden, voor het bedrijf, en vooral voor de klant zelf. *“U wilt toch niet dat anderen zomaar bij uw gegevens kunnen?”*

Geef alternatieven. Later bellen, online via een portal, of in persoon. **Even goede vrienden**, dat is de toon die werkt. Met wederzijds respect en wederzijdse voorbereiding. En als gezamenlijke doel: de klant veilig en efficiënt helpen.

Veelgestelde vragen over klantverificatie (FAQ)

Hoe verloopt het verificatieproces in de praktijk?

Het verificatieproces verloopt in stappen waarbij eerst basisgegevens worden gevraagd, gevolgd door aanvullende controles afhankelijk van het verzoek.

Stappen: Eerst worden basisgegevens gevraagd: naam, geboortedatum. Daarna volgen aanvullende controles, afhankelijk van het verzoek. Bij eenvoudige vragen volstaan die basisgegevens. Bij wijzigingen met financiële impact worden extra methoden ingezet, een code die gestuurd wordt per e-mail of sms, bijvoorbeeld.

Welke gegevens vraagt een bedrijf tijdens verificatie?

Een bedrijf vraagt alleen wat noodzakelijk is: naam, geboortedatum, postcode, huisnummer en een identificerend nummer zoals klant- of polisnummer.

Een bedrijf verzamelt alleen wat noodzakelijk is. De meest gebruikelijke gegevens: naam, geboortedatum, postcode met huisnummer. Een identificerend nummer (klant-, contract- of polisnummer) als dat redelijk past bij het verzoek. Bij betalingen kunnen de laatste cijfers van een IBAN worden gevraagd. Een instantie verzamelt nooit volledige wachtwoorden of complete bankrekeningnummers.

Kan ik klantverificatie automatiseren in mijn contactcenter?

Ja, veel processen kun je automatiseren via login-systemen, automatische codes, DigiD of iDIN, maar persoonlijke hulp blijft belangrijk bij complexe verzoeken.

Veel processen kun je automatiseren: verificatie via login-systemen, codes die automatisch gestuurd worden, koppeling met DigiD of iDin. Automatiseren maakt het sneller en vermindert fouten. Maar persoonlijke hulp of toelichting blijft belangrijk bij complexe verzoeken waarbij je alternatieven moet kunnen bieden.

Als we het hebben over ‘live klantcontact’ lijkt volledige automatisering van klantidentificatie, niet aan de orde. Er zijn wel middelen die het proces efficiënter maken (zie hierboven). Er zullen weinig experts meer zijn, die nummerherkenning als verificatie zullen aanbevelen. Dat is bewezen kwetsbaar.

Wat een goed voorbeeld is van 100% automatisering, zijn online portals of apps waarin de klant inlogt en zichzelf identificeert. Als hij, eenmaal ingelogd, vanuit dat portal live contact zoekt, kan verdere verificatie veelal achterwege blijven bij reguliere klantvragen. Helaas zie ik te vaak dat contact beperkt blijft tot contactformulieren of een chatbot (al dan niet offline) en dat calls niet tot de contactmogelijkheden behoren. Jammer, want vanaf mijn smartphone is dit toch zeker een prima mogelijkheid.

Wat zijn de beschikbare methoden om klanten te verifiëren?

Beschikbare methoden zijn: login-verificatie, tweefactorauthenticatie, iDIN/DigiD, telefonische vragen, fysieke verificatie, virtuele verificatie en terugbellen.

Er zijn meerdere beschikbare manieren:

- Verificatie via account-login op website of app
- Tweefactorauthenticatie met een code per e-mail of sms
- Verificatie via iDIN (internetbankieren) of DigiD bij de overheid
- Telefonische verificatie met persoonlijke vragen
- Live verificatie bij een fysieke locatie
- Virtuele verificatie met meerdere selfies en kopie identiteitsbewijs
- Verificatie via bekende contactgegevens (terugbellen naar geregistreerd nummer)

Hoe help ik klanten die geen gegevens bij de hand hebben?

Leg vriendelijk uit welke gegevens nodig zijn, maak een unieke code voor het verzoek, of verwijs naar de portal of een e-mail vanaf bekend adres.

Als je klanten hebt die onvoorbereid bellen, bied dan alternatieven. Leg vriendelijk uit welke gegevens je nodig hebt en waarom. Geef aan waar ze die online of in documenten kunnen vinden. Maak een unieke code aan zodat het

verzoek bewaard blijft. Stel voor dat ze de portal openen en hun verzoek indienen. Vraag een e-mail te sturen vanaf een bekend e-mailadres met de nodige gegevens. Het gaat erom dat je meedenkt.

Moeten we voor elk verzoek dezelfde voorschriften hanteren?

Nee, controles moeten proportioneel zijn: basisgegevens voor informatie, strengere checks voor contractwijzigingen, extra stappen voor financiële transacties.

Dus voorschriften en controles moeten redelijk en proportioneel zijn. Voor een informatievraag volstaan basisgegevens. Voor contractwijzigingen zijn strengere checks nodig. Voor financiële transacties zijn extra stappen verplicht. Belangrijk is: per type verzoek duidelijke richtlijnen hebben, zodat medewerkers weten welke methode ze moeten toepassen.

Wat moet ik doen als klanten verificatie frustrerend vinden?

Leg vooraf uit waarom gegevens nodig zijn (bescherming), toon empathie, en bied alternatieven. De ergernis daalt van 70% naar 40% bij goede uitleg.

Als verificatie frustrerend overkomt, ligt het vaak aan onduidelijke communicatie. Leg vooraf uit waarom je bepaalde gegevens nodig hebt. Dat het in hun belang is. Wees transparant. Geef alternatieven als ze nu niet voorbereid zijn. Door empathie te tonen – en uit te leggen dat je hen wil beschermen – verminder je weerstand aanzienlijk.

Kunnen we verificatie volledig digitaal laten verlopen?

Ja, voor veel verzoeken via portals en apps met verificatiecodes, maar sommige verzoeken vragen nog steeds persoonlijk contact of fysieke aanwezigheid.

Voor veel verzoeken kan verificatie volledig digitaal: met portals, apps en verificatiecodes. Dat is veiliger en efficiënter. Soms vraagt een verzoek toch om live contact of persoonlijke aanwezigheid. Vaak bij identiteitsdocumenten. Steeds meer verzoeken kunnen digitaal. Toch hebben andere verzoeken nog steeds een persoonlijke touch nodig.

Hoe verstrekken klanten veilig klantgegevens tijdens verificatie?

Klanten moeten gegevens alleen via beveiligde kanalen verstrekken: nooit wachtwoorden of volledige banknummers, altijd via https en tweestapsauthenticatie.

Klanten moeten gegevens alleen verstrekken via beveiligde kanalen. Bij telefonisch contact vraag je nooit om wachtwoorden of complete bankrekeningnummers. Bij online verificatie gebruik je beveiligde verbindingen (https) en tweestapsauthenticatie. Maak klanten bewust van risico op phishing. Vertel dat je bedrijf nooit ongevraagd om gevoelige data vraagt via e-mail of onveilige kanalen.

Waar kunnen we ons verificatieproces verbeteren?

Breng het huidige proces in kaart, noteer waar weerstand ontstaat, train medewerkers, informeer klanten vooraf, en start met kleine verbeteringen.

Begin met je huidige proces in kaart te brengen:

- welke gegevens vraag je nu in klantcontact en waarom (5x)?
- Noteer waar verificatie misgaat en wanneer je weerstand ervaart. Hoe komt dat?
- Heb je uniforme richtlijnen per type verzoek?
- Is verificatie onderdeel van een checklist in contactregistraties?
- Train je medewerkers.
- Monitor de frequentie en resultaten van de klantverificatie;
- Creëer al dan niet als tijdelijke KPI als de situatie daarom vraagt.
- Geef feedback op dit onderdeel van klantcontact.

Informeer klanten vooraf over de verificaties die ze mogen verwachten en waarom via je website en andere contactmomenten.

Start klein met verbeteringen. Breidt dit geleidelijk uit naar geavanceerdere verificatiemethoden zoals automatische codes of portal-verificatie.

Verder lezen?

- Autoriteit Persoonsgegevens: regels voor vaststellen identiteit
- Identificatie en verificatie van persoonsgegevens
- 7 Methods to Verify the Identity of Your Callers

“Elke dag scherper, beter, klantgerichter.” Met SteinBlogs.com.

English Summary

Customer Verification: A Necessary Balance Between Convenience and Security

This article explores why customer verification in contact centers is essential for protecting both businesses and consumers. While digital convenience has made it easier than ever to reach companies through multiple channels, this accessibility paradoxically increases risks of fraud and identity theft. The author distinguishes between customer identification, data verification, and customer verification—the latter being the focus of confirming that the person making contact is genuinely who they claim to be.

The piece argues that asking for customer information isn't bureaucratic hassle but rather customer-friendly protection. Just as we accept showing passports for flights or receipts for returns, providing a policy number or contract details when calling about services is reasonable. The article emphasizes mutual responsibility: customers should prepare when initiating contact, while companies must be transparent about why they need certain information and what they'll never request (like passwords or complete bank details).

Seven practical recommendations guide contact centers toward better verification: inform customers beforehand about needed information, explain the reasoning briefly, offer alternatives when customers lack required data, maintain consistent processes across all channels, and match verification intensity to request complexity. The key message is that customer verification is genuinely customer-friendly when properly explained, balancing ease of access with security through clear communication, empathy, and mutual respect. The goal is helping customers safely and efficiently while protecting their interests.

Resumen en Español

Verificación de Clientes: Un Equilibrio Necesario entre Comodidad y Seguridad

Este artículo explora por qué la verificación de clientes en los centros de contacto es esencial para proteger tanto a las empresas como a los consumidores. Aunque la comodidad digital ha facilitado más que nunca contactar con las empresas a través de múltiples canales, esta accesibilidad aumenta paradójicamente los riesgos de fraude y robo de identidad. El autor distingue entre identificación del cliente, verificación de datos y verificación del cliente—siendo esta última el enfoque principal para confirmar que la persona que contacta es realmente quien dice ser.

El artículo argumenta que solicitar información del cliente no es burocracia molesta sino protección favorable al cliente. Al igual que aceptamos mostrar pasaportes para vuelos o tickets para devoluciones, proporcionar un número de

póliza o detalles del contrato al llamar sobre servicios es razonable. El texto enfatiza la responsabilidad mutua: los clientes deben prepararse al iniciar contacto, mientras que las empresas deben ser transparentes sobre por qué necesitan cierta información y qué nunca solicitarán (como contraseñas o datos bancarios completos).

Siete recomendaciones prácticas guían a los centros de contacto hacia una mejor verificación: informar previamente a los clientes sobre la información necesaria, explicar brevemente el razonamiento, ofrecer alternativas cuando los clientes carezcan de datos requeridos, mantener procesos consistentes en todos los canales y ajustar la intensidad de verificación a la complejidad de la solicitud. El mensaje clave es que la verificación de clientes es genuinamente favorable al cliente cuando se explica adecuadamente, equilibrando la facilidad de acceso con la seguridad mediante comunicación clara, empatía y respeto mutuo. El objetivo es ayudar a los clientes de forma segura y eficiente mientras se protegen sus intereses.