



SkrittLotto

Systembeskrivelse – fra skritt til trekning

Dette dokumentet beskriver hvordan SkrittLotto er bygget: hvordan skritt telles, hvordan lodd oppstår og sendes inn, hvordan dataene beskyttes, og hvordan trekning og vinnerverifisering fungerer. Det er skrevet for deg som vil forstå systemet – enten du er pilotbruker, jobber med folkehelse, eller bare er nysgjerrig på hva som skjer under panseret.

Versjon 8.0
11. juli 2026

App v1.10.0
Android · Kotlin

Nettside v6.47
skrittlotto.no

Enhetstestet
grønn CI på hver endring

Ideen – og rammen rundt piloten

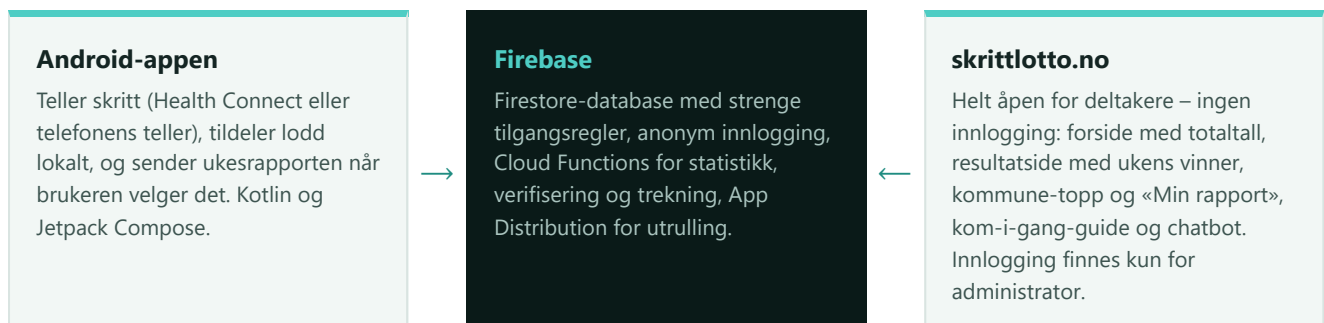
SkrittLotto belønner daglig fysisk aktivitet med lodd til en ukentlig trekning. Regelen er enkel og lik for alle: går du 5 000 skritt i løpet av en dag, får du ett lodd. Maks ett lodd per dag, maks sju per uke. Innsatsen er aldri penger – bare bevegelse.

5 000 SKRITT = 1 LODD	7 MAKS LODD PER UKE	0 kr I INNSATS – ALLTID	søndag UKENTLIG TREKNING
---------------------------------	-------------------------------	-----------------------------------	------------------------------------

Viktig å vite: dette er et proof of concept. SkrittLotto er foreløpig testet i det små – blant venner og familie. Ingen tilknytning til Norsk Tipping, ingen pengeinnsats – ingen reelle premier. Premiepotten og kommunestatistikken i appen er illustrasjoner av hvordan konseptet ville sett ut i full skala. Målet er å vise at ideen bærer, gjennom en app som føles ferdig, og en skrittelling som er til å stole på. Skulle konseptet noen gang realiseres, bygges systemet på nytt med profesjonell drift.

Systemet i ett blikk

Tre deler samarbeider: Android-appen (der skritt telles og lodd oppstår), Firebase (skyen som lagrer innsendinger) og nettsiden (statistikk, resultater og vinnerverifisering).

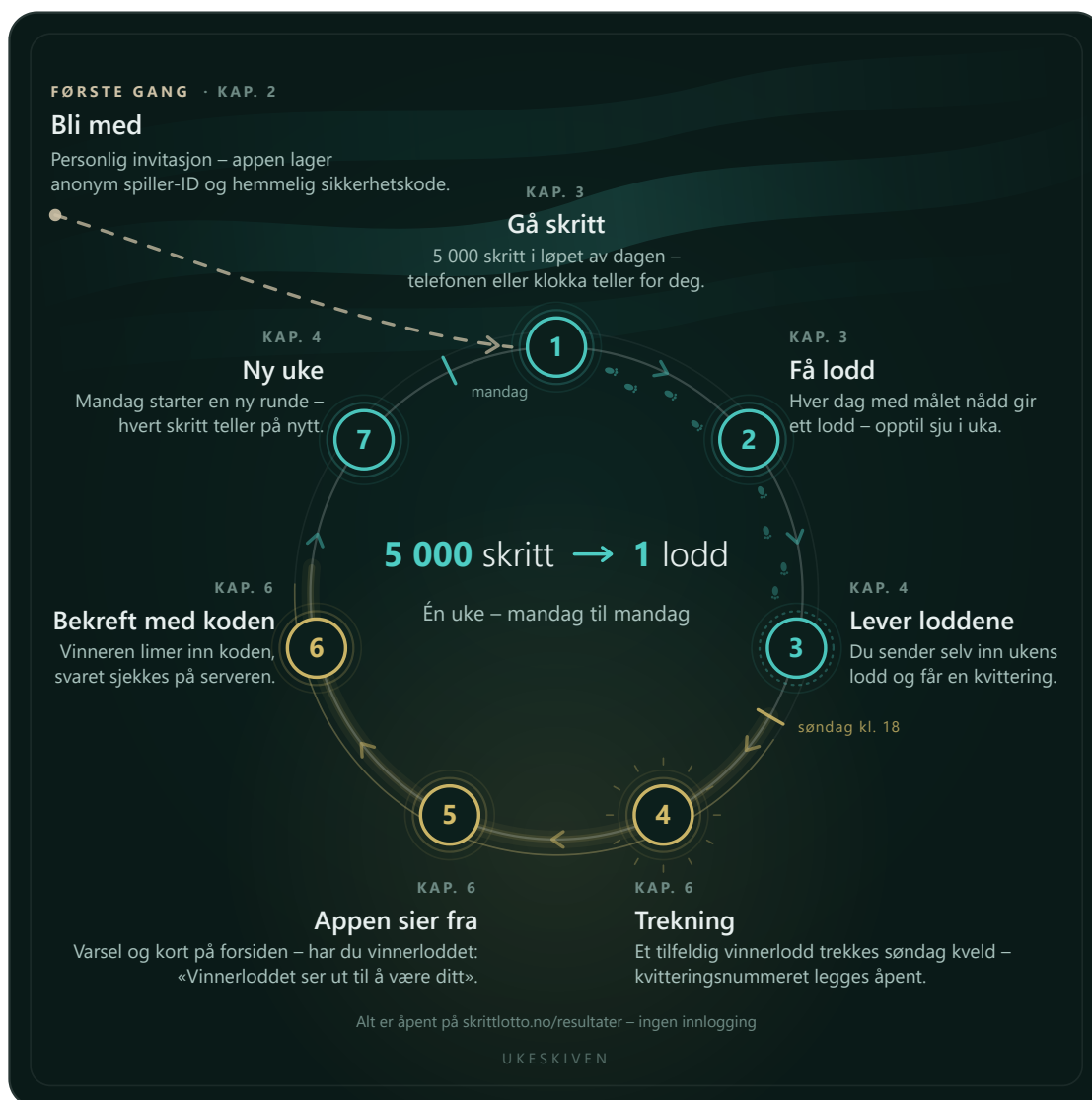


Prinsippene bak

- **Skrittellingen skal være korrekt.** Det er kjernen i hele konseptet: et lotteri der loddet er bevegelse, står og faller på at tallet stemmer. Kapittel 3 beskriver hvordan.
- **Personvern som utgangspunkt.** Brukeren er anonym som standard, styrer selv hva som deles, og den hemmelige sikkerhetskoden bor bare på brukerens egen telefon.
- **Ærlighet i feilsituasjoner.** Når noe ikke kan gjennomføres – ikke nett, rapport avvist, kilde utilgjengelig – sier appen det som det er, på rolig norsk.

Livsløpet til et lodd

Et lodd lever i én uke – fra mandag til mandag. Skritt blir til lodd på telefonen, loddene sendes inn som en ukesrapport, og søndag kveld møter rapporten trekningen. Figuren under følger hele løpet gjennom uka.



● uka di · ● trekningen · ● første gang

Proof of concept: ingen pengeinnsats – ingen reelle premier i pilotfasen.

Identitet, installasjon og **distribusjon**

To nøkler – én offentlig, én privat

Ved første oppstart lager appen to identifikatorer som lagres i telefonens lukkede lagringsområde:

IDENTIFIKATOR	FORMAT	ROLLE
Spiller-ID (offentlig)	SL- + 8 heksadesimale tegn	Brukerens anonyme «kupongnummer» i systemet. En vinner annonseres med kvitteringsnummeret (kapittel 6) – aldri navn, og spiller-ID-en vises ikke.
Sikkerhetskode (privat)	UUID – 36 tegn (32 heksadesimale)	Vinnerbeviset. Bor kun på telefonen; rapporten bærer bare en SHA-256-hash (et énveis «fingeravtrykk») av den. Ved gevinst limer vinneren selv koden inn til sjekk på serveren (kapittel 6).

I tillegg logger appen seg automatisk inn med **Firebase Anonymous Authentication**: skyen tildeler installasjonen en anonym bruker-ID (`firebaseUserId`) uten at brukeren oppretter konto. Denne ID-en er det tilgangsreglene på serveren håndhever eierskap med.

Distribusjon: invitasjon, ikke app-butikk

Appen distribueres som signert APK via **Firebase App Distribution** – ikke Google Play. Installasjonslenken ligger ikke åpent på nettet: lenken *er* invitasjonen, og deles alltid person til person, på to måter:

- **Fra en deltaker:** en eksisterende bruker deler appen rett fra delingsarket – som QR-kode en venn skanner, eller som lenke via systemets delemeny.
- **Via e-post:** har du ingen deltaker å få appen fra, sender du en e-post og får invitasjonslenken tilsendt direkte fra administrator.

Installasjonen krever nettilgang og en Google-konto (kan opprettes på enhver e-postadresse). Nye versjoner rulles ut ved at testerne får varsel fra App Distribution.

Hva skjer ved telefonbytte?

Ingenting av spilldata forlater telefonen – heller ikke via skyen: appen er bevisst unntatt Androids sikkerhetskopiering, slik at «lagres kun lokalt» er bokstavelig sant og sikkerhetskoden aldri kopieres ut av enheten. Profilen (navn, avatar, spiller-ID, sikkerhetskode og skritthistorikk) følger derfor *ikke* med til en ny telefon – bytte eller tap av telefon gir en blank start i piloten. Det er en bevisst beslutning. Sensor-bokføringen har i tillegg en egen vakt: en markørfil som aldri sikkerhetskopieres avslører gjenoppretting, og appen nullstiller da alt som hører til den gamle telefonens fysiske teller.

Appen har også en synlig «gjenopprett med sikkerhetskode»-seremoni. I piloten er den **simulert** – den viser hvordan gjenoppretting ville føltes i et ferdig produkt, men henter ikke reelle data og overskriver ingenting.

Skrittellingen – hjertet i systemet

To kilder, ett tall

Brukeren velger datakilde i Personvern-skjermen, eller lar appen velge automatisk:

- **Health Connect** – Androids helsedata-nav, for de som har klokke eller pulsband (Garmin, Fitbit, Samsung m.fl.). Fordi flere apper kan skrive skritt til Health Connect samtidig, har appen en *kildevelger*: brukeren peker ut hvilken app som skal telle, og aggregeringen filtreres på den. Det fjerner den klassiske feilen der klokke + telefon summeres til 30 % for mye.
- **Telefonens teller** – drives av Recording API i Google Play services der det finnes: systemet teller da døgnet rundt, uavhengig av om appen kjører, og overlever omstart. På telefoner uten Play services brukes råsensoren direkte som reserveløsning. Brukeren ser ikke forskjellen.

Løftene tallet holder

LØFTE	HVORDAN DET HOLDES
Aldri bakover	Dagens tall kan bare øke. Eneste unntak er når brukeren selv velger en ny Health Connect-kilde og tallet korrigeres ned til den kildens fasit – en bevisst, synlig handling.
Kildebytte teller videre – aldri dobbelt	Bytter man kilde midt på dagen, bevares dagens tall og den nye kilden teller videre derfra. Mot Health Connect måles «videre» fra selve byttetidspunktet – slik at en klokke som synkroniserer hele dagen i etterkant ikke får skrittene før byttet talt to ganger.
Tapte dager hentes inn	Både Health Connect og Recording API har historikk. Åpnes appen etter noen dagers pause, fylles hullene, og reelle 5 000-dager i innværende uke får loddene sine i etterkant.
Teller uten at appen er åpen	En bakgrunnsjobb synkroniserer hver halvtime og kan tildele lodd og gratulere – med Health Connect-bakgrunnstillatelse der systemet støtter det.
Robust mot omstart og telefonbytte	Omstart oppdages ved at sensoren hopper bakover, og opptjente skritt bevares i et eget regnskap. Grunnverdier settes aldri til 0 – «vet ikke ennå» er en egen tilstand, slik at telefonens totalteller aldri feiltolkes som dagens skritt.
Midnatt er trygg	Hele synkroniseringskjeden – telling, loddtildeling, streak og feiring – deler én og samme dato, bestemt når kjeden starter. En sync som krysser midnatt kan derfor ikke gi lodd for den nye dagen.

Ærlighet om måling

Ingen skritteller er perfekt: telefoner teller gjerne litt for lavt (de ligger iblant stille på bordet), mens klokker kan telle litt for høyt (husarbeid og håndbevegelser). Appen sier dette rett ut i kildevelgeren, og lar brukeren velge kilden som følger dem tettest. Manuelt innskrevne skritt i Health Connect trekkes bevisst *ikke* fra i piloten – da ville appens tall avveket fra Health Connect-appens eget, noe som ser ut som en tellefeil.

Lodd, innsending og datakontrakten

Fra skritt til lodd

Lodd tildeles lokalt på telefonen i det dagens tall passerer 5 000. Hver dato kan bare gi ett lodd – settet med opptjente datoer gjør dobbelttildeling umulig. Et opptjent lodd trekkes aldri tilbake, og dagen beholder plassen sin i brukerens «streak» (sammenhengende dager med målet nådd) selv om tallet senere korrigeres ned.

Innsending av ukesrapporten

Deltakelse i trekningen krever en aktiv handling: brukeren sender inn ukens rapport fra hovedskjermen, styrt av enkle kjøreregler:

REGEL	INNHold
Oppdateringsfrekvens	Rapporten kan oppdateres hver 6. time – men sperren nullstilles øyeblikkelig ved nytt lodd.
Smart-sjekk	Er ingenting endret siden sist, sier appen fra i stedet for å sende identiske data på nytt.
Stengetid	Søndag kl. 18.00 til mandag kl. 08.00 er innsending stengt, slik at trekningsgrunnlaget er i ro.
En rapport per uke	Dokument-ID-en er <code>spillerID_ukestart</code> – å sende på nytt oppdaterer samme dokument, dupliserer aldri.

Brukeren bestemmer hva som deles

Innsendingsdialogen har brytere for navn, kommune og skritthistorikk – alle av som standard – og det brukeren ser i dialogen er nøyaktig det som sendes. En ny bruker sender «Anonym bruker» og kun ukesummen; navn, kommune og dag-for-dag-historikk følger bare med ved aktivt valg.

Ukesrapporten – felt for felt

Rapporten har tolv felter, og serverens tilgangsregler avviser alt som mangler felter, har feil type eller bryter grensene:

FELT	INNHold OG GRENSE
<code>playerId</code> / <code>firebaseUserId</code>	Spiller-ID (mønsteret <code>SL-...</code> håndheves) og anonym eier-ID, som må tilhøre avsenderen
<code>weekStartDate</code>	Ukens mandag som dato, innenfor rimelig årstall-spenn
<code>ticketDates</code> / <code>totalTickets</code>	Datoene loddene ble opptjent og antallet (0–7) – antallet må stemme nøyaktig med antall datoer, og hver dato valideres som gyldig ISO-datoformat
<code>dailySteps</code> / <code>weeklyStepsTotal</code>	Dag-for-dag-skritt (maks 7 dager; tomt hvis historikkdeling er av) og ukesummen, som alltid sendes ($\leq 1\,000\,000$)
<code>userName</code> / <code>municipality</code>	Navn og kommune – eller «Anonym bruker» / «Privat»
<code>securitySignature</code>	SHA-256-hash av sikkerhetskoden, nøyaktig 64 tegn
<code>receiptId</code> / <code>timestamp</code>	Kvitteringsnummer (<code>KV-...</code> , deterministisk – se kapittel 6) og innsendingstidspunkt

Kontrakten er «låst» i begge kodebaser: endres et felt i appen, må reglene på serveren oppdateres først – ellers avvises innsendingen.

Skyen, reglene og nettsiden

Nettsiden er helt åpen for deltakere: ukens vinner, kommune-toppen og «Min rapport» ligger offentlig på `skrittlotto.no/resultater`; innlogging finnes kun for administrator.

Hvem får gjøre hva i databasen

Firestore-reglene (strammet kraftig i juli 2026) er systemets dørvakt:

- **Ingen kan lese andres rapporter.** Oppslag krever eierskap, «list alle» er stengt, og «Min rapport» går via en serverfunksjon som fjerner sensitive felter.
- **Ingen kan overskrive andres rapporter.** Oppdatering krever eierskap. Etter reinstallasjon (ny anonym ID) er ukens rapport derfor låst – appen sier da ærlig at «ukens lodd ble sendt inn fra en tidligere installasjon».
- **Innholdet valideres på serveren.** Alle tolv felter sjekkes for type og grenser (kapittel 4). Avvises innholdet, skiller appen dette fra «låst» og sier det som det er.
- **Statistikk kan ikke manipuleres.** Totaltallene eies av en serverfunksjon; ingen klient får skrive dem.
- **Vinnerdataene er stengt for alle klienter.** Nettsiden leser kun et sanert, offentlig vinner-øyeblikksbilde – signaturen forlater aldri serveren.

Serverfunksjonene (Cloud Functions)

FUNKSJON	GJØR
<code>onReportWritten</code>	Regner om global statistikk og kommune-aggregater hver gang en rapport lagres – til offentlig lesbare, skrivebeskyttede samlinger – og holder vinner-øyeblikksbildet ferskt.
<code>getPlayerReports</code>	«Min rapport»-oppslaget på den åpne resultatsiden – sanert, uten signatur og eier-ID, med dagstak.
<code>verifyWinnerCode</code>	Vinnerverifisering: hasher den innlimte koden og sammenligner med signaturen – på serveren, med dagstak på forsøk (kapittel 6).
<code>onWinnerWritten</code>	Skriver det sanerte, offentlige vinner-øyeblikksbildet når en vinner registreres.
<code>getDrawList</code> m.fl.	Trekningspanelets admin-verktøy: loddliste, annonsering, statuslinje, marker og angre (kapittel 6).
<code>rebuildStats</code>	Administratorens «regn alt på nytt»-knapp for statistikken.
<code>chat</code>	AI-chatbot for brukerstøtte på nettsiden, hastighetsbegrenset per bruker.

Krasjrapportering (Crashlytics)

Feiler appen, sendes en anonym krasjrapport til Google (feilinformasjon, enhetsmodell/OS-versjon, teknisk installasjons-ID). Også *håndterte* kjerneflyt-feil rapporteres anonymt («non-fatal»), gjennom et saneringslag som vasker spiller-ID-er, kvitteringsnumre, koder og signaturer ut av meldingene; for fatale krasj hviler løftet på en testvoktet kodenorm – appens egne feilmeldinger bygges aldri av brukerdata. Rapportene inneholder aldri navn, spiller-ID eller sikkerhetskode, og debug-bygg sender aldri.

App-attest (App Check) – i monitoreringsmodus

Appen fester en App Check-attest (Play Integrity) på Firebase-kallene, og nettsiden fester tilsvarende (reCAPTCHA Enterprise, usynlig for besøkende, opplyst i personvernerklæringen) – «ekte app / ekte nettleser»-bevis som ikke bærer spillerdata. Begge kjører i monitoreringsmodus – håndheving er ikke slått på: neste trinn er at backend på sikt kun godtar kall fra den ekte appen og nettsiden.

Trekning, verifisering og **vinner-varselet**

Trekningen: eget panel på nettsiden

Administrator trekker et tilfeldig vinnerlodd blant ukens innsendte lodd, fra et eget trekningspanel på nettsiden (Firebase Console beholdes som reserveløsning). Panelet følger hele livssyklusen:

- **Loddliste og trekk:** ukens nummererte liste – ett nummer per innsendt kvittering – med innebygd tilfeldig trekk.
- **Annonsering:** vinnerloddets kvitteringsnummer annonseres via en serverfunksjon som først kontrollerer at rapporten med nummeret finnes – en tastefeil gir feilmelding, ikke en «ukjent» vinner.
- **Status:** en statuslinje viser hvor saken står – annonsert og venter, vinner bekreftet med koden (med tidspunkt), eller gevinst markert.
- **Marker og angre:** gevinsten markeres som bekreftet når vinneren har meldt seg – og en annonsering kan angres uten at noe går tapt; resultatsiden faller da tilbake til «ikke trukket ennå».

Vinnerverifisering – beviset sjekkes på serveren

Så bevises eierskapet – uten at hemmeligheten noen gang vises offentlig:

- 1 Vinneren finner sikkerhetskoden sin i appen (Profil-skjermen, «Identifikasjon»-kortet) og limer den inn på resultatsiden.
- 2 Kodens sendes til en serverfunksjon som lager SHA-256-hashen og sammenligner med `securitySignature` – på serveren, i rapporten bak det annonserte kvitteringsnummeret; klienten velger aldri hvilken rapport det sjekkes mot. Svaret tilbake er kun ja eller nei – signaturen forlater aldri serveren.
- 3 En vellykket bekreftelse stemples med tidspunkt på serveren, synlig kun for administrator – vinneren trenger ikke gjøre noe mer.

Kvitteringen binder det sammen. Da brukeren sendte inn, fikk hun et kvitteringsnummer i appen – for eksempel KV-2026U28-A1B2C3D4. Det er deterministisk – samme spiller og samme uke gir alltid samme nummer – og det er dette nummeret nettsiden annonserer som «Vinnerlodd», så brukeren kjenner igjen sitt eget lodd. Nummeret vist i appen, lagret i skyen og annonsert på nettsiden er ett og det samme.

Vinner-varselet i appen – og forsidekortet

Appen forteller brukeren når vinneren er annonsert. En bakgrunnsjobb leser det sanerte, offentlige vinner-øyeblikksbildet i faste vinduer – søndag kveld, en daglig morgensjekk og ved app-åpning i samme vinduer; omtrent 7–11 dokument-lesinger per uke per enhet. Varselet kommer rolig på varselkanalen «Trekningen»:

- **Generelt varsel** («Ukens vinner er annonsert») – et trykk åpner resultatsiden.
- **Personlig variant** når vinnerloddet er brukerens eget («🇳🇴 Vinnerloddet ser ut til å være ditt!») – matchet på kvitteringsnummerets hex-hale, så øyeblikksbildet trenger ingen spiller-ID.

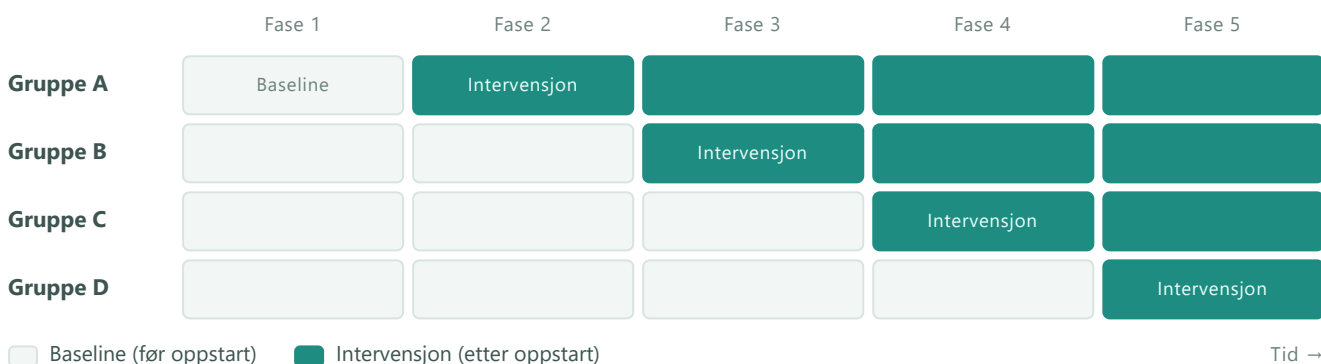
Annonseringen vises også som et rolig gull-kort på appens forside, i generell eller personlig variant, til brukeren lukker det eller det er over en uke gammelt – slik når den også brukere uten varsel-tillatelse. Den personlige viser kvitteringsnummeret, med «Hent koden»-snarvei til profilen. Øyeblikksbildet inneholder aldri navn eller signatur, og appen sender ingenting i denne flyten – den leser bare det som alt er offentlig.

Pilot – og veien videre

Dette er en pilotversjon, laget for å teste hvordan spillmekanismer kan brukes i norsk folkehelsearbeid. Målet er beskjedent: å vise at ideen bærer – en løsning som er enkel å ta i bruk, etisk forsvarlig, og som lar seg måle. Det som følger er ikke løfter, men en skisse av hva et ferdig system kunne blitt, for den som vil se hvor veien går videre.

Slik kan effekten måles

En pilot bør kunne si noe om den virker. En anerkjent tilnærming er *stepped-wedge*- og *multippel baseline*-design: i stedet for å starte alle samtidig, fases tiltaket inn i én gruppe av gangen, til ulike tidspunkt. Da er hver gruppe sin egen kontroll før oppstart, og effekten kan sammenlignes både innen og mellom grupper over tid.



Eksempel på et pilotdesign: intervensjonen fases inn i ulike grupper til ulike tidspunkt, slik at hver gruppe fungerer som sin egen kontroll og effekten kan leses både innen og mellom grupper.

Hvis konseptet skal vokse

Piloten er bygget bevisst enkel. Skal den bli et reelt tiltak, er det noen naturlige neste steg – hvert med sin faglige begrunnelse:

- **Trygg identitet:** BankID sikrer at hver deltaker er unik og hindrer juks med doble kontoer.
- **Sterkere måling:** valgfri validering på selve enheten (uten at posisjon forlater telefonen) og kalibrering mot akselerometer hos et lite utvalg, for å styrke tallenes pålitelighet fra tidlig fase.
- **Åpen, anonym statistikk:** daglig oppdatert kommunestatistikk, vist kun for kommuner med nok aktive brukere til at ingen enkeltperson kan gjenkjennes.
- **Forskningsverdi:** kobling mot nasjonale helseregistre via tiltrodd tredjepart – med analyser på aidentifiserte data – kan måle effekt på sykdomsbyrde, gode leveår (DALYs) og sparte helseutgifter.

Varig, ikke bare i starten

SkrittLotto låner tankegods fra implementeringsvitenskap – fagfeltet for hvordan tiltak faktisk tas i bruk og opprettholdes over tid. Derfor er tiltaket lavterskel og tenkt innført gradvis: testet i liten skala, justert underveis, og enkelt å ta i bruk for både enkeltpersoner og kommuner. Loddet er ment som en startmotor; når vanen sitter, tar bedre søvn og mer overskudd gradvis over som drivkraft.

Personvern, grenser og **kvalitet**

Hva sendes – og hva sendes aldri

- **Sendes (med brukerens valg):** spiller-ID, ukens lodd-datoer, ukesum, kvitteringsnummer, kode-hash, teknisk eier-ID (den anonyme innloggingen) og tidsstempel – og valgfritt navn, kommune og dag-for-dag-historikk (alle av som standard).
- **Sendes aldri:** sikkerhetskoden med rapporten (den bærer kun hashen; ved gevinst limer vinneren selv koden inn til sjekk på serveren) – og posisjon, kamera, mikrofon og kontakter ber appen aldri om. Kontaktinformasjon finnes ikke: ingen kontoregistrering.
- **Lagres kun lokalt:** skritthistorikk (365 dager), profil, innstillinger og all sensor-bokføring. Appen er unntatt Androids skysikkerhetskopi – «kun lokalt» er bokstavelig ment.

Skrittdata leses med brukerens eksplisitte tillatelse via Androids systemdialoger, og appen forklarer på forhånd – på norsk – hvorfor den spør. Utover det spør appen bare om lov til å sende varsler – valgfritt, brukt til påminnelser, feiringer og vinner-varselet.

Kvalitetsarbeidet

- **Enhetstestene tester de ekte klassene** – lagring og sensorer injiseres i testene, slik at logikken som testes er nøyaktig den som kjører på telefonen – og hele suiten kjøres grønn.
- **Kontinuerlig integrasjon:** hver eneste endring som lastes opp til GitHub bygger appen og kjører hele testsuiten automatisk.
- **Krasjovervåkning** via Crashlytics, med lesbare linjenummer beholdt gjennom app-krympingen (R8) – hva rapportene inneholder, og aldri inneholder, står i kapittel 5.
- **Adversariell gransking:** kodebasen leses jevnlig kritisk av uavhengige gransker-agenter – senest 11. juli 2026. Funn verifiseres mot koden, rettes samme dag og dokumenteres i repoets levende arbeidsdokument.
- **Dokumentene vedlikeholdes:** dette dokumentet, designsystemet og teknisk arbeidsliste lever i kodebasen og oppdateres i samme endring som koden – et dokument skal være sant, eller arkiveres.

Kort sagt: SkrittLotto er et lite proof of concept, laget med omhu. Bygget av én produkteier i tett samarbeid med KI-agenter – med testdekning, tilgangsregler og ærlige feilmeldinger som om det skulle i produksjon, og med full åpenhet om hva som er ekte og hva som er en illustrasjon.

Pilotens bevisste grenser

- Premiepott og kommunestatistikk er **illustrasjoner** av konseptet i full skala.
- Gjenopprettings-seremonien er simulert, og telefonbytte gir blank start (kapittel 2).
- Ingen trekningsmotor kjører av seg selv – tilfeldig-trekket i panelet utløses og bekreftes av administrator.

Ved en eventuell realisering må disse bygges på ekte, sammen med blant annet full App Check-håndheving (attestene for app og nettside kjører i dag i monitoreringsmodus – kapittel 5), server-styrt tidsvalidering og en full personvernvrdering – lotteri-lignende tjenester er regulert farvann i Norge.