Det tysta dataläckaget

En granskning av hur Sveriges mest använda och samhällsbärande appar läcker data om sina användare och vilka risker det medför för digital suveränitet, konsumentskydd och nationell säkerhet.

SHIBUYA
PEAK PRIVACY

Det tysta dataläckaget

De flesta av oss använder mobilappar utan att tänka särskilt mycket på vad som händer i bakgrunden. Appar för bank, vård och andra viktiga vardagstjänster upplevs som neutrala hjälpmedel i ett fungerande samhälle. Just därför är denna granskning viktig. När appar i tysthet skickar data vidare utan användarens tillåtelse, och ofta utan att ens apputgivaren har full insyn, uppstår risker som går bortom den enskilda individen. Information om vardagliga beteenden kan i stor skala användas för spårning, profilering och kartläggning.

Men data från appar är dock bara toppen av isberget när det kommer till integritet och säker datahantering. Samma mönster kan skönjas i många företags hantering av sin egna, affärskritiska data. Cyberresiliens handlar ytterst om kontroll, om var den lagras och övervakas. Genom att ta tillbaka kontrollen över datan skapar vi företag och ett samhälle som bättre kan stå emot hotbilder.

VIBEKE SPECHT, PEAK PRIVACY | ANDREAS LUNDGREN, SHIBUYA

PHOTO BY: MARKUS SPISKE ON UNSPLASH

Populära, svenska appar läcker data utomlands – utan samtycke

Vår granskning av de mest använda apparna inom samhällsbärande områden visar att de skickar känslig data till externa aktörer, trots uteblivet samtycke. Data överförs i stor utsträckning till servrar med jurisdiktion utanför EU. Situationen möjliggör kartläggning av rörelsemönster och profilering av enskilda individer, samtidigt som kontrollen över datan förloras.

Granskningen, som genomförts av Peak Privacy och Shibuya, omfattar de 75 mest användarna apparna inom finans, vård, utbildning, hälsa och livsmedel. Totalt skickar 87 procent av apparna data till externa aktörer och 95 procent av dessa överför information till länder utanför EU, framför allt USA och Kanada.

91% av de svenska apparna innehåller inbyggda färdigkomponenter (SDK), kod som ofta är försedda av externa tjänsteleverantörer, som lever inuti appen och ofta delar den åtkomst till användarens enhet som appen själv har. I genomsnitt innehåller varje svensk app närmare 14 sådana komponenter.

Finans och hälsa utmärker sig som de kategorier som gör flest anrop och innehåller flest komponenter.

Utbildningsapparna har lägst nivåer av tredjepartskontakt men även där skickas majoriteten av datan till mottagare utanför EU.

Datan kan användas för att följa individers rörelser över tid, till exempel personer med roller där spårning kan utgöra en säkerhetsrisk, exempelvis militär personal, vårdpersonal eller offentliga befattningshavare. Eftersom datan ofta hamnar i system som används i den globala reklamtekniska infrastrukturen finns inga tekniska begränsningar som hindrar vidare spridning eller lagring.

Granskningen visar att dessa dataflöden förekommer brett i svenska appar och att överföringarna kan användas för kommersiell profilering och för att kartlägga användarbeteenden på detaljnivå.

87%

av apparna skickar data till externa aktörer.

95%

av dessa överför information till länder utanför EU.

Så genomfördes granskningen

Granskningen av de 75 svenska mobilapparna bygger på dynamiska tester där apparna används i verkliga scenarier. Metoden gör det möjligt att se vilka externa aktörer som tar emot data och vilka tekniska komponenter som är inbyggda i apparna.

Arbetet genomfördes genom att varje app laddades ner, installerades och användes i en kontrollerad testmiljö medan all nätverkstrafik dokumenterades. Om en app bad om informerat samtycke tackade testmiljön nej för att synliggöra hur de fungerar utan godkännande. Detta gav en bild av vilka nätverksanrop som sker när det saknas samtycke.

Analysen identifierade mottagare för varje datapaket, deras geografiska placering och vilken typ av data som skickades. Granskningen kartlade också inbyggda tredjepartskomponenter, så kallade SDK:er, och vilka åtkomsträttigheter de delar med appen, såsom platsdata eller kameraåtkomst.

Peak Privacy använder denna metodik för att mäta vad appar faktiskt gör i drift jämfört med vad integritetspolicyn beskriver. Genom dynamisk testning och teknisk loggning går det att se dataflöden som normalt inte syns för användaren och att bedöma hur omfattande kontakterna med externa aktörer är.

Resultatet har sedan analyserats av Peak Privacy tillsammans med Shibuyas informationssäkerhetsexperter. Den samlade granskningen och analysen ger både en teknisk helhetsbild av hur svenska appar arbetar i praktiken, vilka dataöverföringar som sker vid vanlig användning och vilka risker det medför.

Vad är det för data som skickas vidare?

När mobilappar kommunicerar med externa företag skickas mer än anonym teknisk information. En granskning av nätverksanrop visar att data som kan användas för att identifiera och följa enskilda användare över tid regelbundet överförs till analys- och reklamföretag.

Utöver SDK- och nätverksanalysen har vi för ett urval appar även analyserat innehållet i de faktiska dataöverföringarna. Genom att analysera innehållet i apparnas nätverksanrop, den så kallade payloaden, går det att se vilken typ av data som faktiskt skickas från användarens enhet. Vår kontroll visar att överföringarna ofta innehåller detaljerad teknisk och beteendebaserad information.

Ett konkret exempel kommer från en av de mest använda svenska vårdapparna, där data skickades till ett amerikanskt analysföretag. I kommunikationen ingick ett beständigt enhets-ID, iOS IDFV, som skapas av Apple på telefonen, läses ut av appen och skickas vidare till mottagaren. Ett sådant ID gör det möjligt att särskilja och känna igen samma enhet vid upprepade tillfällen.

Utöver detta skickades uppgifter om användarens land och språk, i detta fall Danmark och svenska, samt information om telefonmodell, operativsystemets version och exakt skärmstorlek. Tillsammans med tidsstämplar på millisekundnivå och uppgifter om vad användaren gjorde i appen, exempelvis att trycka på logga ut-knappen, skapas ett detaljerat mönster av användarbeteendet.

Vissa av uppgifterna, som enhets-ID, är direkta identifierare. Andra, som telefonmodell och skärmstorlek, delas av många användare var för sig. Men i kombination kan de bli unika och bilda ett så kallat fingeravtryck av enheten. Det gör det möjligt att identifiera en användare även utan ett beständigt ID.

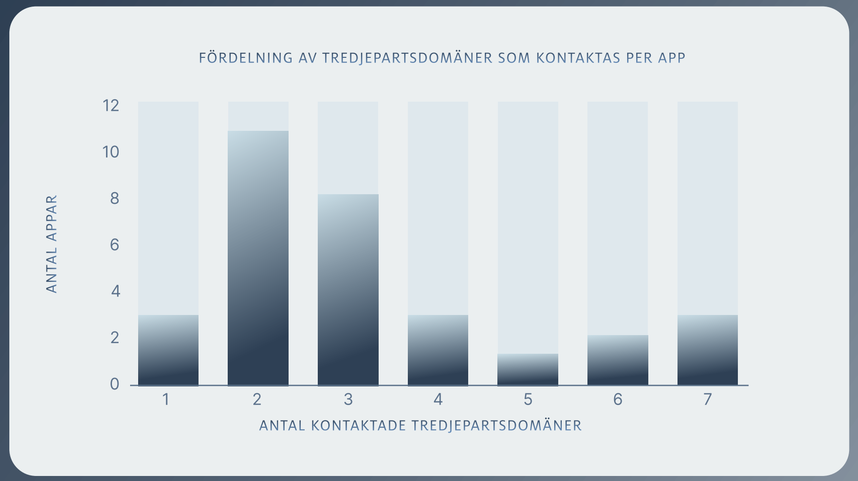
Ett beständigt enhets-ID klassas som en personuppgift enligt GDPR eftersom det gör det möjligt att spåra samma användare över tid och att bygga mer detaljerade profiler. När denna tekniska information kombineras med beteendedata, som exakt vad en användare gör och när, förstärks möjligheterna ytterligare.

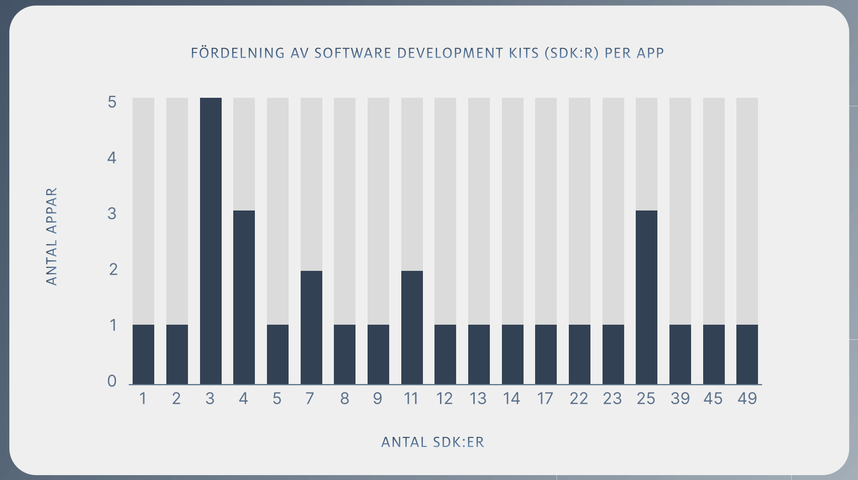
Finansappar

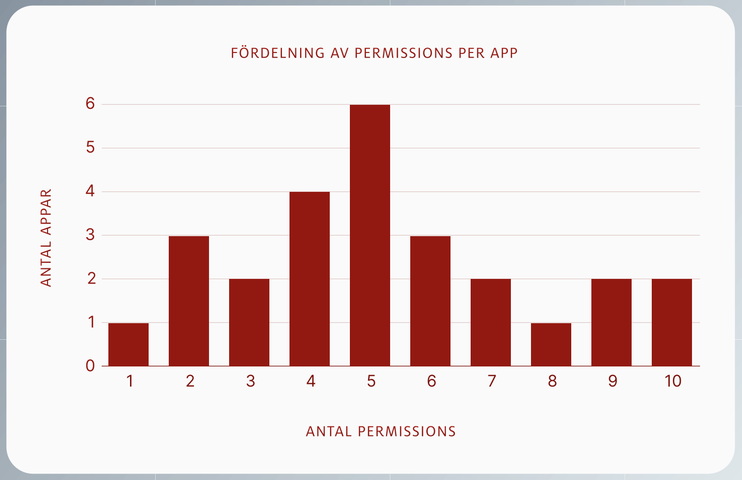
I granskningen analyserades 31 svenska finansappar. Resultatet visar att samtliga skickar användardata till externa mottagare, och att majoriteten överför information till servrar utanför EU.

Apparna testades genom dynamisk körning där de användes i praktiska scenarier samtidigt som all nätverkstrafik loggades. Samtliga 31 gjorde tredjepartsanrop och alla utom en (1) skickade data till mottagare i USA eller Kanada.

29 av 31 innehåller SDK:er, med ett genomsnitt på drygt 13 tredjepartskomponenter per app.





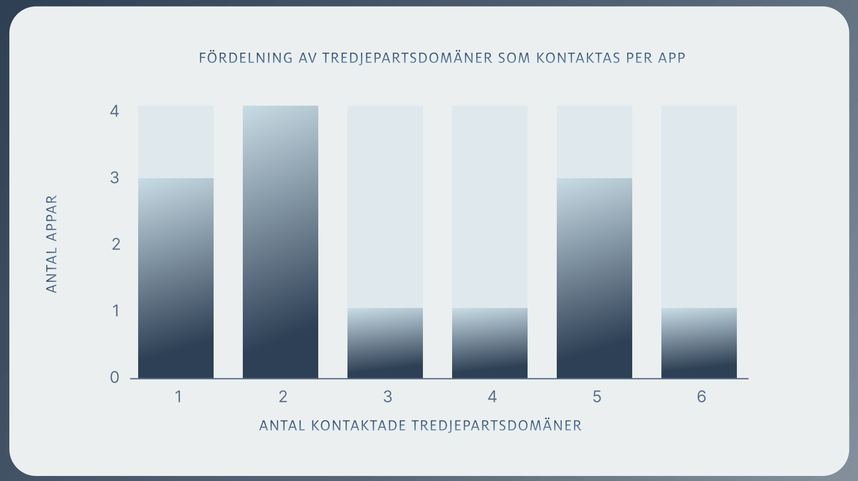


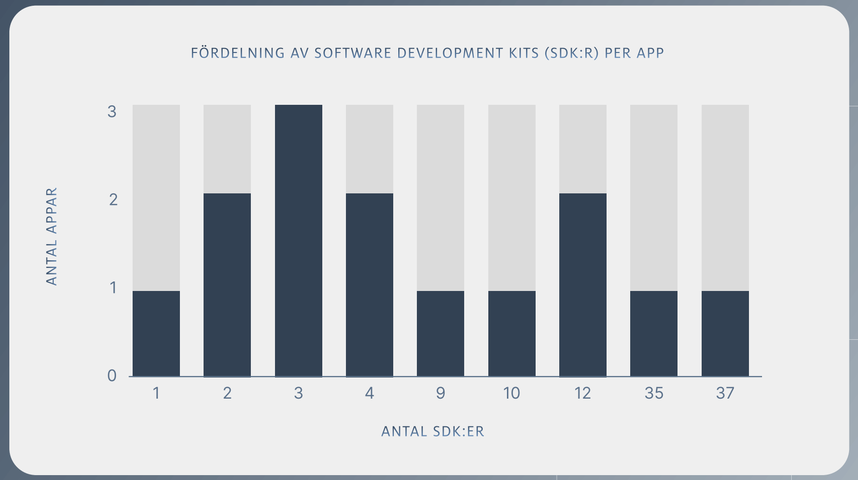
Vårdappar

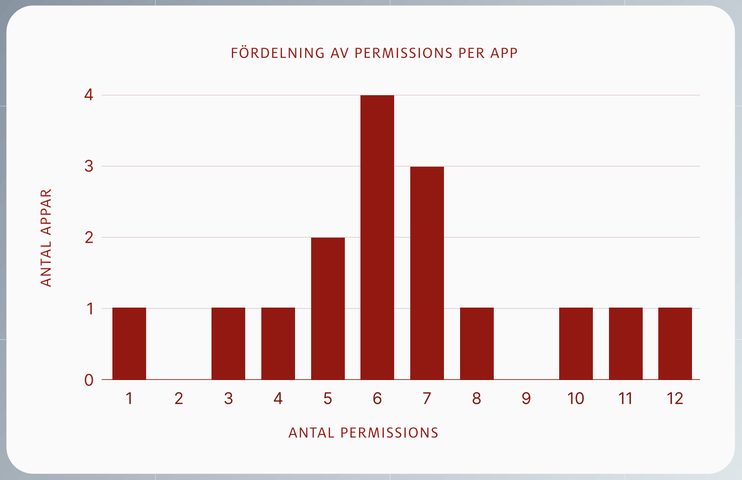
I granskningen av svenska mobilappar analyserades 16 appar inom vårdkategorin. Resultatet visar att 13 av dem skickar användardata till externa mottagare.

Alla utom en (1) skickade data till mottagare i USA eller Kanada.

I genomsnitt identifierades drygt tre tredjepartsförfrågningar per app, som dessutom i genomsnitt innehåller nästan 10 SDK:er.





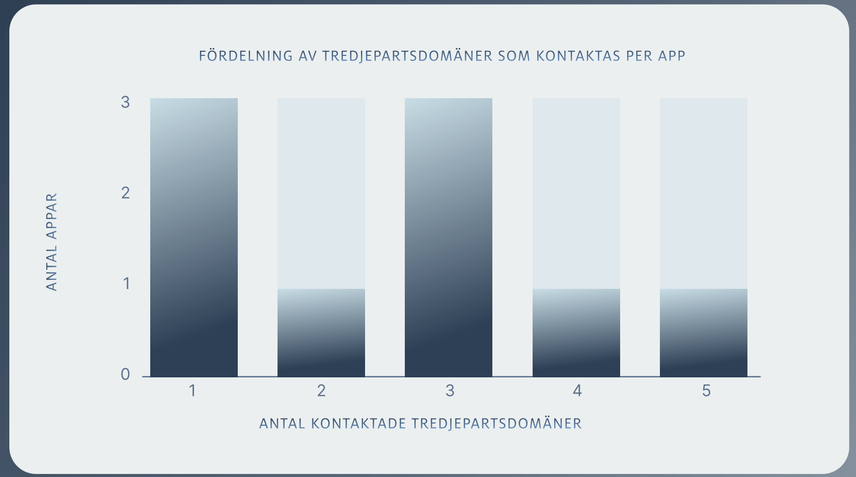


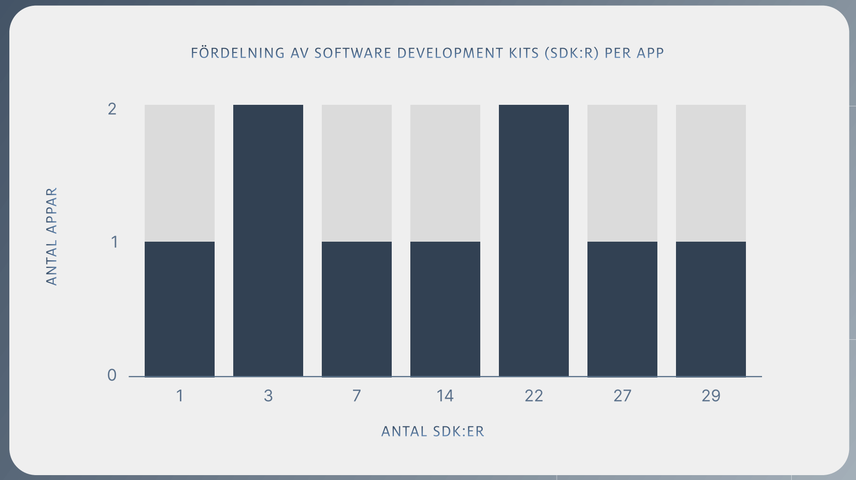
Hälsoappar

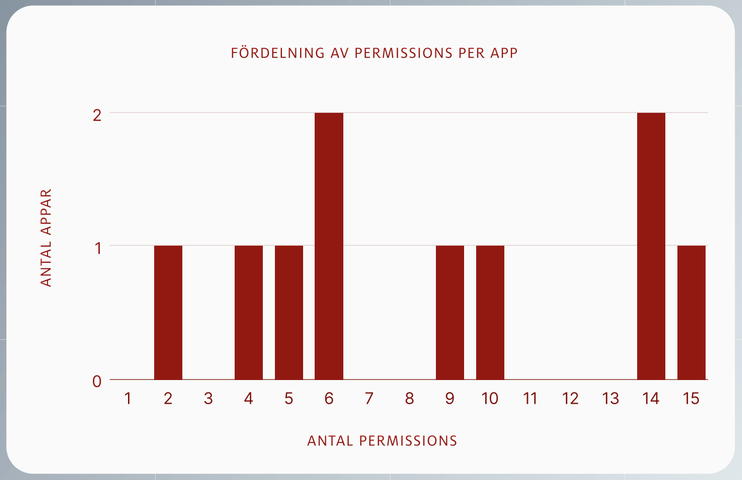
Totalt analyserades 10 appar inom kategorin hälsa och träning.

Av dessa gjorde 9 appar tredjepartsanrop, varav samtliga skickade data till servrar utanför EU, främst i USA och Kanada. I genomsnitt registrerades cirka 2,6 tredjepartsförfrågningar per app.

Samtliga appar innehöll SDK:er, i genomsnitt över 14 stycken per app.







*En av apparna i den här kategorin har 83 sdk:er vilket påverkar genomsnittet. Notera dock att denna app inte är en del i uträkningen av snittet.

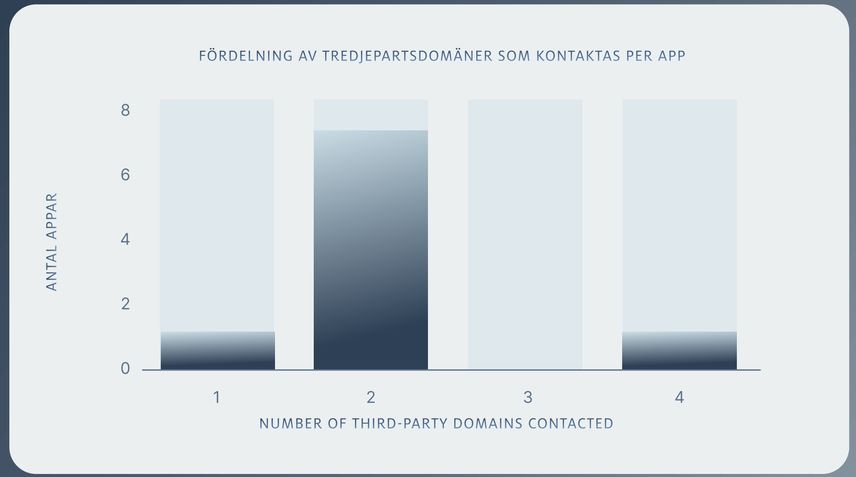
Utbildning

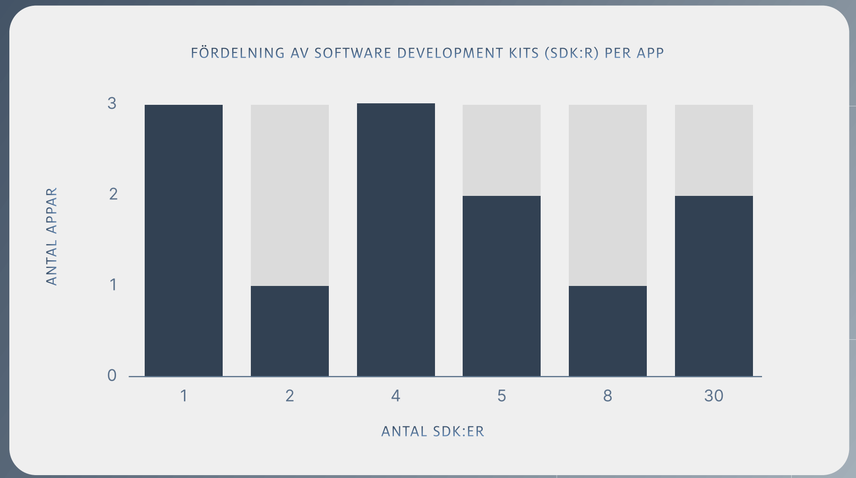
I utbildningskategorin analyserades 15 appar som används i skol- och studiemiljöer. Resultaten visar att tredjepartskontakter är mindre vanliga än i andra kategorier men fortfarande förekommer.

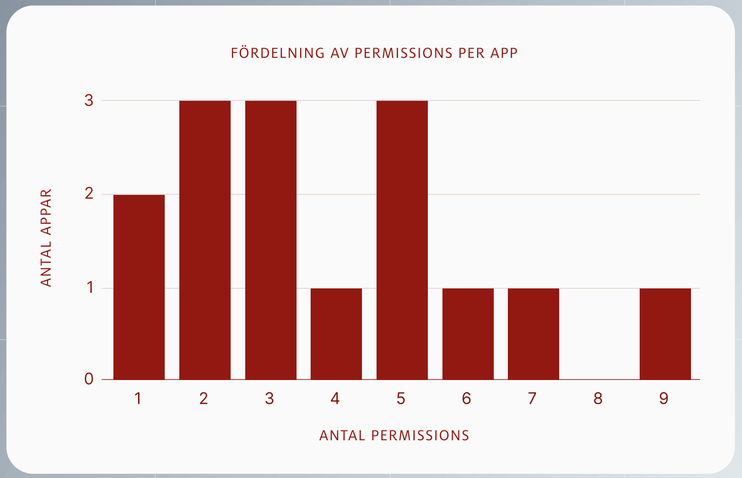
Av de 15 utbildningsapparna gjorde 9 appar tredjepartsanrop till externa mottagare. Åtta av dessa skickade data till servrar utanför EU.

I genomsnitt noterades drygt två tredjeparts-förfrågningar per app.

Utbildningsapparna innehöll i genomsnitt drygt åtta SDK:er per app.







Livsmedelsbranschen

Livsmedelskategorin är den minsta i granskningen men visar entydiga resultat. Totalt analyserades tre av de mest nedladdade apparna i kategorin och samtliga gjorde tredjepartsanrop och skickade data till mottagare utanför EU.

Appar i kategorin hade i genomsnitt 23 tredjepartskomponenter (SDK), vilket är högst av alla kategorier i granskningen.

3/3

appar skickar data till externa aktörer.

0

appar använder cookies.*

23

SDK:er i snitt per app.

6,67

permissions per app.

*Cookies är inte lika vanligt förekommande som spårningsmetod i mobila applikationer som på webbplatser.

Så används svenskarnas appdata i reklamindustrins maskineri

Vet du vad din app gör bakom kulisserna? Den som publicerar en mobilapp bär det juridiska ansvaret för allt som sker i den. Men den som tjänar pengar på upplägget är inte främst appägaren. Det är den globala adtechindustrin.

"Adtechindustrin är på väg att passera en biljon dollar. Den bygger på att samla in så mycket data som möjligt, från så många källor som möjligt, och just mobilappar är en av de största källorna. Det har aldrig legat i den industrins intresse att vara transparenta kring detta", säger Vibeke Specht, medgrundare till Peak Privacy och författare till boken "From GDPR Confusion to Privacy First Marketing".

För en apputvecklare eller appägare blir det som att köpa grisen i säcken, berättar hon. Ett kodpaket för kraschrapportering låter ofarligt. Men även det skickar typiskt enhetens IP-adress, enhetsidentifierare och tidsstämplar till leverantörens servrar varje gång appen startas. Inte bara när den kraschar. Och leverantören råkar kanske vara ett av världens största annonsföretag.

"De använder sen datan för att bygga detaljerade användarprofiler. Ju fler datapunkter, från fler appar, desto mer värdefulla blir profilerna för deras annonsekosystem. Så står du där och har just kopplat in din app i en global adtechmarknad, utan att du kanske ens är medveten om det."

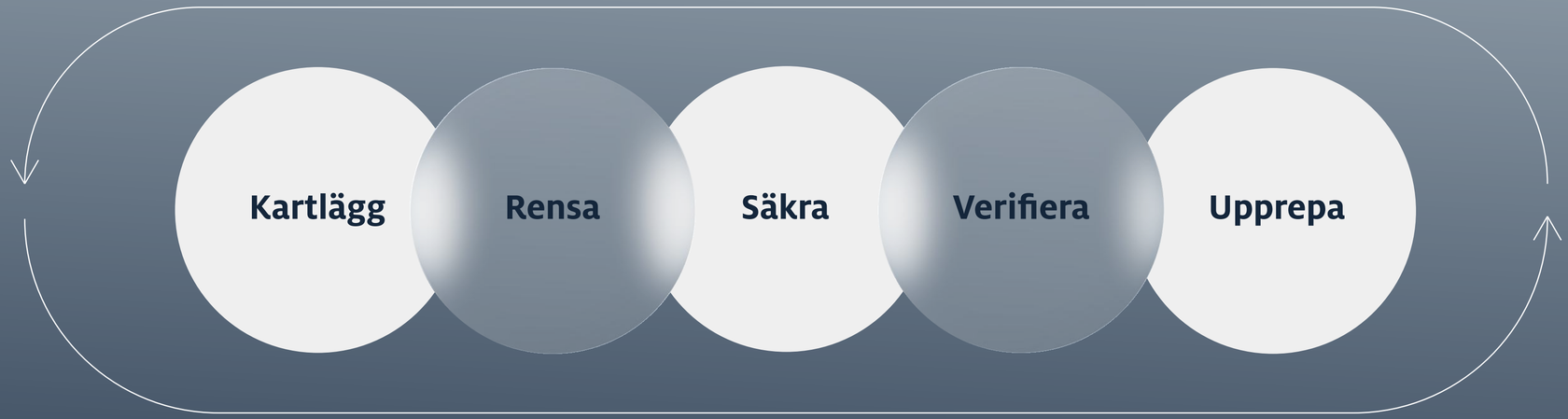
Men det stannar inte vid reklam. Dataförmedlare paketerar och säljer datan vidare. Köparna kan vara övervakningsföretag, underrättelseaktörer, eller vem som helst som är villig att betala. Ingen hackning behövs. Det visade till exempel Le Mondes granskning i början av 2026.

"Så detta rör inte bara dataskydd. En app som läcker data är också en app som kan läcka information om din organisation. Lagstiftning som NIS2 kräver att du hanterar risker i hela
din leverantörskedja, och en tredjepartstjänst som din app kommunicerar med är en underleverantör. Att inte veta vad den gör är i sig en brist i riskhanteringen."

Så sent som i april 2026 bötfällde den italienska dataskyddsmyndigheten ägarna till två bankappar med sammanlagt över 12,5 miljoner euro. Orsaken: ett enda SDK, ursprungligen avsett för bedrägeribekämpning, vars datainsamling bedömdes som oproportionerlig.

"Och så finns kostnaden som ingen pratar om. Varje onödig tredjepartsrelation är ett avtal att underhålla, en konsekvensbedömning att göra, en attackyta att bevaka. Att rensa bort det som inte behövs ger en säkrare produkt och lägre förvaltningskostnader."

> **”Att rensa bort det som inte behövs ger en säkrare produkt och lägre förvaltningskostnader.”**
>
> VIBEKE SPECHT, PEAK PRIVACY



KARTLÄGG

Se appen i skarpt läge, som en användare använder den. Vilka externa parter kontaktas? Vilka komponenter (SDK:er) är inbyggda? Vilka åtkomster till mobiltelefonens funktioner begärs av appen? Fungerar samtycket som det ska?

(Samma kartläggning ger underlag som organisationen ändå behöver för t.ex. GDPR, ePrivacy, NIS2, ISO 27001 och SOC 2.)

RENSA

Utgå från kartläggningen och fråga vad som behövs för appens syfte? Ta bort det som inte kan motiveras. Varje onödig SDK är en risk.

SÄKRA

Uppdatera integritetspolicy så att den speglar vad appen faktiskt gör. Behåll bara det du kan stå för.

VERIFIERA

Testa, mät och bekräfta att insamling och delning faktiskt stoppas när användaren avböjer. Ett nej ska vara ett nej, inte bara en knapp i gränssnittet.

UPPREPA

Appen förändras vid varje uppdatering. Nya paket ger nya beroenden och nya flöden. Gör kartläggning och kontroll löpande, inte som en engångsinsats.

När appdata blir en verksamhetsrisk

Mobilapparnas dataflöden är inte enbart ett integritetsproblem för individen, de innebär också en konkret risk för varje organisation. Samma tekniska infrastruktur som används för kommersiell profilering kan också användas för att kartlägga verksamheter, rutiner och affärskritisk information.

I början av 2026 publicerade den franska tidningen Le Monde en granskning som visade hur platsdata från reklamindustrin kunde användas för att identifiera anställda vid känsliga verksamheter – utan att något system behövde hackas. Informationen var lagligt köpt från en dataförmedlare och tillgänglig på den öppna marknaden.

I mars 2026 kunde data från en träningsapp dessutom avslöja positionen för det franska hangarfartyget Charles de Gaulle.

“Exemplen är extrema, men den underliggande mekanismen är densamma för alla verksamheter. Det handlar om system som är byggda för massinsamling av data och som därmed också kan användas för kartläggning av alla typer av organisationer”, berättar Andreas Lundgren, ansvarig för compliance och security på Shibuya.

Han menar också att platsdata inte behöver vara exakta GPS-koordinater. När återkommande positioner, tidsstämplar och stabila identifierare kombineras räcker det för att fastställa var någon arbetar, vilka rutiner de har och vilka lokaler de besöker regelbundet.

"Det gäller inte bara säkerhetskänslig verksamhet – det gäller alla företag med information värd att skydda", säger Andreas Lundgren.

Frågan sträcker sig längre än integritet och samtycke. Den berör informationssäkerhet och organisationers förmåga att skydda sin verksamhet, sina anställda och sin konkurrenskraft.

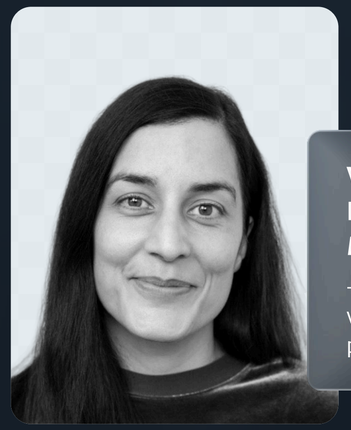
Även dataöverföringsavtal mellan Europa och USA spelar in. Befintliga ramverk för dataskydd förändrar inte det faktum att utländsk lagstiftning kan ge myndigheter möjlighet att begära ut data från bolag under deras jurisdiktion.

“Cyberresiliens handlar ytterst om kontroll: Vilka appar får medarbetare använda på arbetsenheter? Vilka riktlinjer finns för privata enheter som används i tjänsten? Hur hanteras data som genereras i det vardagliga arbetet och vilken data lämnar verksamheten via de enheter och appar som används varje dag? Det behöver adresseras systematiskt, inte app för app”, säger Andreas Lundgren.

SHIBUYA
BY PULSEN

Andreas Lundgren
Compliance & Security

+46 707 93 14 58
andreas.lundgren@shibuya.se
shibuya.se



PEAK PRIVACY

Vibeke Specht
Dataskyddsspecialist
Medgrundare Peak Privacy

+45 21 33 31 47
vibeke@peakprivacy.eu
peakprivacy.eu