The silent data leak

How mission-critical apps in Sweden and Scandinavia transmit data beyond all control – and why it matters to every organization

A report on how the global advertising industry's infrastructure has been woven into Sweden's most widely used mobile applications, why this constitutes a structural threat to data protection, digital sovereignty, national security, and your organization's information security – and what you can do about it.

Contents

Executive Summary

We have examined 188 mobile applications across the finance, healthcare, education, health and grocery sectors on the Scandinavian market. Seventy-five of these are offered on the Swedish market.

87 percent of the Swedish apps initiate network connections to external companies despite consent having been denied or never requested. Ninety-five percent of these connections are made to service providers outside Europe, primarily in the United States and Canada. Each app contains, on average, more than thirteen embedded code packages developed by other companies. Among grocery apps, the average is 23.

The review is based on dynamic testing. Each app was installed, launched and used under realistic conditions while all communication with external parties was logged. When an app requested consent, the test system declined. We measured what the app actually does, not what its privacy policy claims it does.

These are not obscure niche applications. They include banking and payment apps that millions of Swedes are likely to open every day, healthcare and health apps that process sensitive information, and grocery apps found in virtually every household.

Within the finance category, all reviewed Swedish apps transmit data to third parties. Within health, all apps contain embedded components developed by external companies.

For your organization, this is two issues—not one.

The first concerns the applications you publish yourselves. As the publisher, you bear the legal responsibility — including for components and data flows over which you have no direct visibility. The second concerns the applications your employees carry with them. On corporate devices and private devices used for work, the same apps covered by this review are present. The same building blocks. The same uncontrolled data flows. When aggregated, these flows reveal where your employees are located, how the organization operates, which individuals move together, and when activity increases in unusual locations. This is business information leaving the organization without any explicit decision having been made.

This is not merely a data protection issue. It is an operational risk.

Each embedded component both shares the app's permissions on the device and may contain vulnerabilities that can be exploited to access data in other applications. This applies to both iOS and Android. Findings to this effect have been published by, among others, Microsoft and Indiana University.

This is not an isolated incident. When consumer apps and enterprise apps coexist on the same device, every uncontrolled app becomes part of the attack surface against the organization's information.

The problem is structural. The key question is not whether a single organization has acted incorrectly, but why the ecosystem is designed in a way that makes individual actors "get it wrong." And, crucially, what you can do about it.

Reduce risk

1. Gain visibility — conduct an independent dynamic assessment to determine how applications behave in real-world use, in the hands of an actual user. This applies to all applications within the organization, both those you publish and those used by employees on corporate mobile devices.
2. Minimize risk — make informed decisions on remediation measures based on the assessment, in order to reduce risk, strengthen regulatory compliance, and improve security.
3. Act and verify — once changes have been implemented, it must be verified that the risk has in fact been reduced. This is done by repeating steps 1 and 2.

1. About the review

This report is based on an analysis of 188 mobile applications across five categories. All applications were downloaded from Apple's App Store, which dominates the Scandinavian mobile market with a market share of approximately 60 percent in Sweden, 62 percent in Norway, and 57 percent in Denmark.[1]

Selection and scope

The applications represent five categories: finance, healthcare, education, health and grocery. The seclection includes the most widely used applications on the Swedish and Danish markets. By "Swedish apps," we refer to the 75 applications that are actively used on the Swedish market, regardless of whether they are published by a Swedish, Danish or international company.
The reviewed applications represent some of Sweden´s largest actors in banking, education, health, and grocery retail. Collectively, they reach millions of Swedish users.

Now we tested

Each application was tested dynamically. The app was installed, launched, and used under realistic conditions while all communication with external parties was logged.
If the app requested consent for data collection, the test system consistently declined.
If the app did not request consent at all, this was recorded.
Denying consent is a deliberate part of the test methodology. It makes visible what occurs without the user's active approval.

DYNAMIC TESTING VS. STATIC ANALYSIS

Static analysis examines an application's code and configuration. It shows what can happen. Dynamic testing observes the application in operation. It shows what actually happens. An app may, in theory, be correctly configured and still transmit data via SDKs that act independently. Dynamic testing captures this behavior.

What we measure is what the app actually does, not what its privacy policy claims it does. For each app, we map which external companies it contacts, the jurisdictions in which recipients are located, which embedded components (SDKs) the app consists of, which access permissions it requests on the user's device, and whether the consent mechanism functions as stated.

[1] Statcounter GlobalStats. Mobile operating system market s hare in Sweden, Norway and Denmark..

Terminology Used in This Report

When we state that an app "transmits data," we mean that the app makes documented network requests to third-party servers. Each such request exposes, at a minimum, the sender's IP address, which constitutes personal data under EU case law. In addition, advertising and analytics SDKs typically transmit further identifying information, such as device identifiers, technical device information, and timestamps.

WHAT IS AN SDK?

SDK stands for Software Development Kit. It is typically a pre-built code package that an app developer integrates into an application to provide a specific function, such as crash reporting, map services, social media login, or analysis of user behavior.

Each SDK is generally (though not always) code developed by another company that runs inside the app. It shares the app's access permissions, can communicate with its own servers, and can be updated without the app owner actively deciding to do so.

The average app in this review contains more than thirteen such code packages. This means that a typical app is not the product of a single company. It is the product of a dozen.

The source material for this report is based on the analysis documentation of each individual application.

Why SDK-analysis is central in the mobile environment

Cookies are the web's memory. They make it possible for a website, or a third party embedded within it, to recognize the same user over time and across different websites.

In a mobile application, this infrastructure does not exist in the same way. Cookies do occur, primarily when an app loads web content in an embedded view, and we record them when this happens.

In apps, users are identified through the device's own identifiers, through fingerprinting based on hardware and software characteristics, and through the code the app is built from. As this study shows, a significant portion of that code consists of pre-built packages developed by other companies SDKs. Each SDK operates within the app, shares its access permissions, and often communicates with its own servers.

It should also be noted that a developer may introduce vulnerabilities independently, without using an SDK, and without fully understanding the associated risk landscape.

Our review therefore captures both the documented SDKs and the network requests that actually occur, regardless of which code component triggers them.

2. 188 apps, five categories, one pattern

73 percent of the reviewed apps transmit data to external companies without a legal basis. Ninety percent of these transmissions are directed to companies under jurisdictions outside Europe.

Overall results

On average, each app contacts just over three external services. In some categories, the number is higher. Approximately three out of four apps contain embedded pre-built components, with an average of more than thirteen per app. This means that a typical app in this review incorporates code from a dozen external companies into its product—code whose behavior the app owner rarely has sufficient visibility into.

The most common access permissions requested by apps on the user's mobile device relate to location data, camera access, network information, and storage. Each app requests multiple such permissions. Each permission expands the amount of personal data that the app's third-party components may potentially access.

COOKIES PLAY A SECONDARY ROLE IN MOBILE APPS

18 percent of the apps set cookies. This is consistent with the picture presented in the previous chapter. In the mobile app environment, cookies are not the primary mechanism through which tracking occurs. They appear mainly when an app loads web content in an embedded view, but they do not continue to track the user beyond that context within the app.

The Swedish apps perform worse

The Swedish apps perform worse than the Scandinavian average:

- 87 percent transmit data to external companies without a legal basis. This is 14 percentage points above the average for the review as a whole.
- 95 percent of these transmit data to servers outside Europe.
- 91 percent contain embedded pre-built components, with an average of 14 per app.
- Each Swedish app also requests access to multiple functions on the user's device, most commonly location data, camera access, contacts, and storage.

The difference can partly be explained by the fact that the Swedish sample includes a higher proportion of finance apps and more widely used consumer applications.

Resultas by category

Finance

All reviewed Swedish finance apps transmit data to external companies. All but one transmit data outside Europe. These are Sweden's most widely used banking, payment, and investment apps—applications that millions of citizens open every day to manage their finances, and which at the same time, without the user's awareness, deliver data to companies whose business models are based on profiling user behavior.

The finance category is subject to the strictest requirements for data handling and customer trust, yet it also exhibits the highest proportion of apps transmitting data to external parties in this review.

Health

All reviewed health apps contain third-party components, with an average of more than fourteen SDKs per app. One app in the category contains eighty-three such components. Nine out of ten apps contact third parties, and all of these transmit data outside Europe. Health apps also request the highest number of access permissions of all categories. This means that third-party components operating within the app may potentially have access to location data, camera access, and more.

> Consider a menstrual cycle tracking app. If the app sends a network request via an analytics SDK such as Google Firebase Analytics, this is not merely an anonymous ping. The data packet typically includes an IP address, device model, persistent device identifiers, timestamps, and behavioral events such as "cycle day logged" or "symptom reported." In a health application, such data is particularly sensitive. However, the underlying principle applies across all categories.

Grocery

Three apps. Two leading Swedish grocery chains and one fast-growing challenger. Each transmits data to third parties outside Europe. On average, each grocery app contains 23 embedded components—almost twice as many as banking apps. These applications are used by millions of households every week.

Healthcare

The proportion of apps with third-party contact is lower within healthcare: eighty-one percent. This may indicate a greater awareness of data sensitivity. However, eighty-one percent remains high. Of the healthcare apps that contact third parties, ninety-two percent transmit data outside Europe.

Education

Education has the lowest share of third-party contacts in the review: sixty percent. However, among education apps that do have third-party contact, eighty-nine percent transmit data outside the EU/EEA. These apps are used by children and young people. That nearly nine out of ten apps with third-party contact transmit data outside Europe is, in itself, noteworthy.

3. Why It looks this way – and why It matters to your organization

A mobile app appears to be a single product. You download it, open it, and it does what it promises. It shows your bank balance, books a healthcare appointment, counts calories. Beneath its branded surface lies something else: code from a dozen companies, assembled into one product.

How an app is built

An app developer rarely builds an application entirely from scratch. Instead, they rely on pre-built building blocks—code packages developed by other companies. One package to display maps.

One to handle payments. One to measure how users navigate within the app.
As noted in the previous chapter, these packages are referred to as SDKs, Software Development Kits. Each SDK is typically code developed by another company that operates within the app. It shares the app's access permissions. It can communicate with its own servers. And it can be updated without the app owner actively deciding to do so.

The average app in this review contains more than thirteen such code packages. This means that a typical app is not the product of a single company. It is the product of a dozen.

The underlying business logic

Many SDKs are offered to app developers free of charge. The reason is straightforward: the provider monetizes the data the app gives them access to.

This is the same business logic that has driven the surveillance-based advertising industry for two decades—first on the web through cookies, and later in mobile apps through SDKs.

The app developer wants to quickly and efficiently build a functioning app. The SDK provider wants data. Both get what they want. But it is the user who pays, with their information. And it is the app owner who bears the legal responsibility.

This business model stands in direct conflict with the core GDPR principles of data minimization and purpose limitation.

An information security risk — not just a data protection issuea

It would be easy to view this solely as a matter of privacy and data protection. Doing so would underestimate the scope of the problem. Any application that contains third-party components not controlled by the organization constitutes an information security risk in the most fundamental sense of the term.

A mobile application is part of an organization's digital surface. It is an extension of the brand, the customer relationship, and, in many cases, the organization's most sensitive data flows. When an app incorporates a dozen code packages from external companies, without the app owner having insight into what they do beyond accessing the user's camera, location, and contacts, this is not merely a privacy issue. It is a question of which parts of the organization's digital exposure lie outside its control.

DOES NOT AFFEC ONLY SECURITY-SENSITIVE ORGANIZATIONS

Det är lätt att uppfatta risker med okontrollerade dataflöden som något som främst berör myndigheter, försvar och underrättelsetjänst. Men infrastrukturen vi beskriver i den här rapporten gör ingen skillnad mellan en bankapp och en myndighetsapp. Mellan en livsmedelskedja och en försvarsaktör.

Any organization that publishes an app containing third-party SDKs is part of the same ecosystem. Data flows through the same channels, to the same recipients, with the same lack of control.

The risk is multi-dimensional:

- **Information Security**
  Information security is affected by the fact that SDKs, which share the app's access permissions, operate as uncontrolled access points without the app owner having visibility into their behavior. They can collect data, communicate with external servers, and change their behavior between versions.
- **The Supply Chain**
  The supply chain is affected because each third-party SDK is, in practice, a subcontractor operating within the product itself. If an organization does not know how that subcontractor uses the access it has been granted, it falls short of the risk management requirements set out in both NIS2 and ISO 27001.
- **The Brand**
  The brand is affected as customers, supervisory authorities, and business partners increasingly demand digital credibility. An organization that cannot demonstrate control over the data flows of its own applications exposes itself not only legally, but also commercially.
- **Competitiveness**
  KCompetitiveness is affected by the leakage of business-critical information, not only personal data. In many cases, this data can be purchased from a data broker. No hacking is required.

Research from Oxford University showed as early as 2018 that Android apps contained, on average, ten third-party components with tracking functionality, that more than ninety percent of apps contained at least one such component, and that 88 percent transmitted data to companies under the Alphabet corporate umbrella.[2]
A study published the same year found that millions of Android apps transmitted unencrypted user data—such as names, income information, phone numbers, and GPS coordinates—to servers via embedded SDKs.[3]

When an app becomes a gateway to more than it´s own data

There is another dimension of risk that has become increasingly evident in recent security research. An app that incorporates third-party SDKs can, in certain cases, function as an entry point to data belonging to other apps on the same device — including corporate information.

Both Android and iOS are built on a sandbox model. In theory, each app is isolated, and its data should not be accessible to other apps without explicit authorization. In practice, this isolation is not absolute. Security research has repeatedly shown that the model can be breached through vulnerabilities in the operating system, in the app's own code, or — particularly relevant to this report — in the third-party SDKs embedded within the app.

EngageSDK — a recent example

In April 2026, Microsoft's security team published an analysis of a vulnerability in EngageSDK, a widely used third-party SDK for push notifications in Android apps. The vulnerability made it possible for an app on the same device to bypass Android's sandbox and gain access to private data in other apps that had integrated the same SDK.

The scope was significant. More than fifty million app installations were affected, over thirty million of which were cryptocurrency wallets. For these users, the vulnerability entailed potential exposure of wallet data, private keys, and other financial information. Microsoft notes in its report that apps are increasingly reliant on third-party SDKs. This creates extensive and non-transparent dependencie. [4]

[2] Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. & Shadbolt, N. (2018). Third Party Tracking in the Mobile Ecosystem. WebSci 18: ACM Conference on Web Science.
[3] Unuchek, R. (2018). Leaking ads. Kaspersky Lab Securelist.
[4] Microsoft Defender Security Research Team (2026, april). Intent redirection vulnerability in third-party SDK exposed millions of Android wallets to potential risk.

WHAT IS INTENT REDIRECTION?

In Android, apps communicate with each other and with their own components through so-called intents. These are message objects that request an action. When an app sends an intent, it does so using the app's own identity and access permissions.

Intent redirection occurs when a malicious app manipulates the contents of an intent sent by a vulnerable app. The result is that the app executes instructions originating from the attacker, but with its own permissions. This allows the attacker to access data that would otherwise be protected by the sandbox. In the EngageSDK case, the vulnerability resided in an exported component that the SDK automatically added to the app's manifest during the build process—often without the developer being aware of it.

Not an isolated incident

EngageSDK is not an exception. Security research shows that similar weaknesses recur.

As early as 2018, Check Point demonstrated an attack technique known as Man-in-the-Disk, in which apps that store data in Android's external storage can be manipulated by other apps.[5] In 2022, a vulnerability chain was published that made it possible for a malicious app to completely bypass Android's sandbox, read data from apps such as Facebook and WhatsApp, and, in some cases, inject code.[6]

Academic studies have reached the same conclusion. The Android storage model, as it is used in practice by many app developers, leaks sensitive information between apps at a scale that is not the result of isolated bugs, but of structural design choices.

Many of these vulnerabilities have since been addressed by Google and by SDK vendors. However, the point is not to highlight a specific vulnerability. The point is that third-party SDKs have repeatedly proven capable of acting as a bridge between an app's own sandbox and other information on the device—and that app owners rarely have sufficient visibility into the SDKs they embed.

[5] Check Point Research (2018, augusti). Man-in-the-Disk: Attack against External Storage on Android.
[6] Lin, Y. m.fl. (2024). Peep With A Mirror: Breaking The Integrity of Android App Sandboxing via Unprivileged Cache Side Channel. USENIX Security.

This also applies to iOS

It is tempting to assume that these issues are limited to Android. Apple's sandbox model is stricter in several respects, and Apple frequently emphasizes this in its marketing. Research, however, presents a more nuanced picture. The review underlying this report covers iOS applications exclusively.

In 2020, the security company Snyk published an analysis of Mintegral's advertising SDK, which at the time was integrated into more than 1,200 iOS apps in the App Store. The malicious code within the SDK logged URL-based requests made through the app and transmitted the results to a third-party server, potentially including personally identifiable information. The SDK also contained anti-debugging protections that altered its behavior when it suspected it was being monitored—a mechanism that helped it pass Apple's app review process without detection.[7]

On the academic side, researchers at Indiana University and several collaborating institutions demonstrated so-called XARA attacks—Unauthorized Cross-App Resource Access. In these cases, a sandbox-isolated app approved by Apple was able to gain unauthorized access to sensitive data from other apps, including iCloud, email, and banking credentials.[8] In 2022, Microsoft's security research documented an additional sandbox bypass in iOS, iPadOS, and macOS (CVE-2022-26706) that allowed a sandbox-isolated process to circumvent restrictions and execute code with elevated privileges.[9] Similar sandbox breaches have been documented in connection with iOS zero-day campaigns as recently as 2023.

A comparative study by Oxford University and TU Delft of 24,000 Android and iOS apps concluded in 2021 that third-party tracking and the sharing of unique user identifiers were widespread across apps in both ecosystems.[10] Neither platform is clearly superior to the other in terms of privacy. Another study from 2022 examining Apple's App Tracking Transparency found that even after the introduction of ATT, the Google AdMob SDK continued to contact its servers to the same extent as before.[11] **The problem has not disappeared. It has merely become harder to observe from the outside.**

Apple's own developer guidelines are explicit: developers are responsible for all code in their apps, including code written by others. This serves as a reminder that the risk associated with third-party SDKs does not lie with the operating system provider, but with the app owner. Regardless of platform.

[7] Snyk Research Team (2020, augusti). SourMint: Malicious code, ad fraud, and data leak in iOS.
[8] Xing, L. m.fl. (2015). Unauthorized Cross-App Resource Access on MAC OS X and iOS. Indiana University Bloomington. arXiv:1505.06836
[9] Bar Or, J. / Microsoft 365 Defender Research Team (2022, juli). App sandbox escape vulnerability impacting iOS, iPadOS, macOS, tvOS and watchOS (CVE-2022-26706).
[10] Kollnig, K., Shuba, A., Binns, R., Van Kleek, M. & Shadbolt, N. (2021). Are iPhones Really Better for Privacy? Comparative Study of iOS and Android Apps. arXiv:2109.13722
[11] Kollnig, K. m.fl. (2022). Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels. arXiv:2204.03556

What does this means for your organization

Today, the mobile device is one of the most important work tools in many organizations. Employees read email, handle cases, authenticate to business systems, and access corporate information via their mobile phones. On the same device, consumer apps are often also present—banking services, social media, news, health, and grocery apps. Each typically incorporates a dozen third-party SDKs of varying origin and degree of control.

In a BYOD environment, where employees use their personal devices for work, this coexistence is the rule rather than the exception. But even on company-owned devices, it is common for employees to have a mix of sanctioned and unsanctioned apps installed. This means that every uncontrolled app becomes part of the attack surface against the organization's information—not only a risk to individual user privacy.

Industry research confirms this picture. NowSecure has tested 378,000 Android apps and found that 62 percent request one or more dangerous permissions. More than 70 percent of these apps simultaneously transmit sensitive data to tracking domains.[12] Zimperium has reviewed over 54,000 work-related apps and found that 43 percent of the hundred most widely used enterprise apps contain cryptographic weaknesses that expose corporate data to risk.[13] In its BYOD guidance from October 2025, Gartner recommends that organizations integrate mobile app risk intelligence into their device management and be able to filter apps based on the third-party components they contain.[14]

The question is no longer whether an organization's data resides on devices with uncontrolled apps. The question is what those uncontrolled apps can do with the access they have.

[12] NowSecure (2025). Mobile App Privacy Risk Research - Privacy and Permissions Analysis.
[13] Zimperium zLabs (2025). Mobile App Threat Research - Enterprise App Security Report.
[14] Gartner (2025, oktober). Enable BYOD and BYOPC Securely.

The blind spot

It would be simplest to view this as the result of individual actors' mistakes. But the problem is structural.

When a developer integrates an SDK, it is done to enable a specific function—crash reporting, maps, authentication. That the SDK simultaneously collects data and transmits it to the provider's servers, and that this data may then be propagated through chains beyond the visibility of both the developer and the user, is something developers are rarely aware of.

However, lack of awareness does not absolve responsibility.

SDK providers can also change the behavior of their code packages without the app owner taking any active action. With each update, new data-collection capabilities may be introduced. As a result, an app that was compliant at launch is not necessarily compliant six months later. A version that does not collect location data may be replaced by one that does. A configuration that is disabled at installation may be enabled in a subsequent update.

It is therefore not sufficient to review an app once. The situation can change with every release. And it is only when the app is in operation, in the hands of real users, that its actual behavior can be revealed.

In 2025, CNIL, the French data protection authority, noted that even if a user has granted an app access to, for example, location data, this does not mean that all of the app's SDKs are authorized to use it.[15] Legally, they are not permitted to do so. Technically, they may be able to. This makes the issue one of compliance.

The result is a situation in which the party publishing the app bears full legal responsibility for everything that occurs within it, while in practice lacking visibility into what the app actually does in real-world use. This is what we refer to as the blind spot.

This is not a matter of a few irresponsible actors. Our review shows that the pattern recurs across the majority of the apps we examined, including apps from some of Sweden's most established banks, healthcare providers, and grocery chains. It is a structural problem.

[15] CNIL (2025). Recommandation relative aux applications mobiles. Commission nationale de l'informatique et des libertés.

4. From app to auction

The SDKs we identify in Swedish apps are not isolated components. They are connection points into the global digital advertising industry's infrastructure—a system designed to collect, distribute, and monetize personal data at scale.

The ad auction no one sees

> Imagine logging into your banking app in the morning. At the same time, in the background, an embedded analytics SDK sends a request to its servers. The data packet carries your IP address, device model, a persistent device identifier, a timestamp, and a behavioral event. You see none of this. The bank likely does not see it either. But a company on the other side of the Atlantic does.

Each time an app displays an advertisement, a data packet is sent to hundreds of companies. The packet may include the user's demographic information, browsing history, location, the page being loaded, IP address, device identifiers, timestamps, and technical device information. Every company participating in the auction receives the packet—not only the winner, but all bidders.

Google's technical documentation confirms that 1,102 separate companies can receive data from Google's European auctions. The corresponding figure for Microsoft is reported to be 1,647. This means that a single ad impression may potentially expose user data to more than a thousand recipients.[16]

WHAT IS REAL BIDDING (RTB)?

RTB is the dominant technology for programmatic advertising. The entire process takes place in under one hundred milliseconds—from the moment an app signals available ad inventory to the moment an advertisement is displayed.

The scale is massive. In the United States alone, RTB advertising spend amounted to approximately USD 57 billion in 2023, up from USD 23.5 billion in 2018. This is an infrastructure with strong commercial incentives to participate, which helps explain why SDKs connected to it are so deeply integrated into the app ecosystem.

The issue is not a lack of encryption in transit. The problem lies elsewhere. Once a bid request has been broadcast, there is no technical mechanism that prevents recipients from storing, copying, or further distributing the data. No digital locks. No acknowledgements that guarantee deletion.

DIt is akin to broadcasting a radio program. You cannot technically control who records it. This has been confirmed by 27 European data protection authorities and by the UK Information Commissioner's Office (ICO).[17]

[16] Google, "Ad technology providers". För Microsoft: PDF
[17] Information Commissioner's Office (2019). Update report into adtech and real time bidding.

Not just advertising

A banking app or a healthcare app typically does not display advertisements. It does not participate as a publisher in RTB auctions. Yet it may still feed data into the same infrastructure, primarily through embedded SDKs.

SDKs from Google, Meta, and other actors whose core business is programmatic advertising collect and report data to their own servers regardless of whether the app itself displays ads. A banking app using Google Firebase Analytics communicates with Google's servers. A health app incorporating a Facebook SDK reports into Meta's ecosystem. These ecosystems are RTB ecosystems.

The purpose of the app is irrelevant to the SDK. The SDK does what it is designed to do. The SDKs we identify in Swedish apps largely belong to these very actors.

No way back

Every company that receives a bid request adds the new information to the profile it already holds about the individual concerned. This trade is not merely a mechanism for displaying advertisements. It is a system for the continuous accumulation of personal data, across a large number of actors, without the data subject's visibility.

According to the Irish Council for Civil Liberties, RTB data about individuals in Europe is broadcast 71 trillion times per year. Amazon and Meta are not included in this figure, as comparable data for them is not available.

The right to have one's data erased is central to the GDPR. It presupposes knowing where the data is held. In the RTB system, this prerequisite is structurally impossible to meet. An individual requesting erasure cannot identify the hundreds or thousands of companies that have received data about them. The app owner is unlikely to be able to do so either.

Not just any data — including sensitive categories of personal data

This is not only about IP addresses and device identifiers. In its investigation, the UK data protection authority, the ICO, found that companies within the RTB ecosystem collected and traded information relating to, among other things, race, sexual orientation, health status, and political affiliation—without the consent of the affected users.

This is not ordinary personal data. Under the GDPR, information concerning health, ethnic origin, sexual orientation, and political opinions constitutes so-called special categories of personal data under Article 9.

These categories are subject to stricter rules, require explicit consent as a legal basis, and may not, as a rule, be processed unless specific exemptions apply. That the RTB system in practice processes and trades precisely these categories constitutes a breach of the core principles of European data protection law.

The supervisory authorities´verdict

In February 2022, the Belgian Data Protection Authority ruled that IAB Europe's Transparency and Consent Framework—the framework that authorizes the majority of RTB within the EU—violates the GDPR on multiple points. The decision has been described as "an atomic bomb" for the industry.

Academic commentators have argued that RTB, in its current form, would require a fundamental restructuring in order to comply with the GDPR at all. Since then, the Dutch Data Protection Authority has indicated that actors in the Netherlands should cease using RTB to profile users.

The infrastructure to which Swedish apps currently feed data is therefore operating in a legal context where its authorization within the EU is being questioned by supervisory authorities in multiple Member States..

Academic analyses suggest that a solution that preserves the business model in its current form is unlikely to be achievable within the framework of the GDPR.

From advertising to mapping

The consequences of the RTB system extend beyond advertising. An investigation by the ICCL shows that it enables the purchase of access to specific categories of individuals: military personnel; employees in the defense and aerospace industries; judges and decision-makers within national security. In one of the analyzed documents, access to the category "Government, Intelligence and Counterterrorism" is sold for sixteen European countries. Sweden is one of them.[18]

In January 2026, Le Monde published an investigation based on RTB data purchased from a data broker. The journalists identified home addresses and daily routines of employees of France's foreign intelligence service, the DGSE. They mapped personnel at the nuclear submarine base at Île Longue. They identified members of the security detail protecting President Macron.[20]

The Israeli company ISA has developed a surveillance tool called Patternz which, according to the company itself, has profiled five billion devices through analysis of RTB data. The tool delivers an individual's current location, historical movement patterns, and daily contacts.[21] The information does not originate from government registers. It originates from the advertising industry's ecosystem.

[18] Ryan, J. & Christl, W. ([2023]). Europe's Hidden Security Crisis: How data about European defence personnel and political leaders flows to foreign states and non-state actors. Irish Council for Civil Liberties.
[20] Untersinger, M. & Leloup, D. (2026, januari). How French spies, police and military personnel are betrayed by advertising data. Le Monde.
[21] ICCL, Europe's Hidden Security Crisis (Ryan & Christl 2023). ISA:s Patternz-verktyg beskrivs med hänvisning till företagets egen produktsida, arkiverad av ICCL

The advertising industry's own audience categories reveal more than movement patterns. They include codes indicating whether an individual has recently lost a close relative, has high alcohol consumption, suffers from mental health issues, or is experiencing financial distress.[22] The information is not stolen. It is classified, packaged, and available for purchase. It is precisely the type of information intelligence services use to recruit or coerce individuals.

In 2025, the US data company Gravy Analytics was affected by a data breach. Hackers published more than thirty million location data points on a Russian criminal forum.[23] Gravy Analytics collected a significant portion of its location data through the RTB system. The leaked material revealed location data points from the White House, the Kremlin, the Vatican, and military bases around the world.[24] Weeks before the breach, the Federal Trade Commission had prohibited Gravy Analytics from collecting and selling Americans' location data without consent.[25]

IT IS NOT ONLY ABOUT DEFENSE

These examples involve intelligence services and military bases. But the infrastructure makes no distinction. The same types of data—location information, device identifiers, and behavioral patterns—are collected from all apps within the ecosystem.

A grocery app with twenty-three SDKs feeds data into the same system as a defense-related app. A menstrual cycle tracking app reports to the same servers as a banking app. What makes the military examples striking is that they have been brought to light, not that they are unique.

Any organization that publishes an app containing third-party components whose behavior it does not control participates in the same ecosystem. The question is not whether your organization is affected, but whether you have visibility into how.

Digital souvereignty

95 percent of the Swedish apps that transmit data to third parties send it to companies under jurisdictions outside the EU/EEA. The primary destinations are the United States and Canada. This is not only a legal issue. It is a sovereignty issue.

The US CLOUD Act grants US authorities the right to request access to data held by companies under US jurisdiction, regardless of where the server is physically located. Data about Swedish users, stored by a company under US jurisdiction, may therefore be accessible to US authorities without Swedish authorities being informed.

This is the case despite the existence of a data-sharing agreement between the EU and the United States, the Data Privacy Framework.

[22] ICCL, Europe's Hidden Security Crisis (Ryan & Christl 2023). ICCL hänvisar till IAB Audience Taxonomy och IAB Content Taxonomy som de standardiserade system inom vilket dessa kategorier är kodade och tillgängliga för köp.
[23] Whittaker, Z. (2025, 13 januari). A breach of Gravy Analytics' huge trove of location data threatens the privacy of millions. TechCrunch.
[24] Techcrunch - A breach of Gravy Analytics' huge trove of location data threatens the privacy of millions.
[25] Federal Trade Commission (2024, december). FTC Order Will Ban Venntel and Gravy Analytics from Selling Sensitive Location Data.

> Concrete consequence: After the International Criminal Court issued arrest warrants against Israeli leaders, the Court President's Microsoft account was blocked as a result of political pressure from the United States. An international judicial institution lost access to its own communications because its infrastructure was controlled by a company under the jurisdiction of another state.

The Swedish apps we have reviewed communicate with servers operated by global platform providers, primarily US-based companies. These actors control the infrastructure. They set the terms. They determine where data is stored, for how long, and under what circumstances it is disclosed. This means that decisions with direct implications for the privacy of Swedish citizens and for organizations' digital exposure are made by companies whose primary loyalty does not lie with Swedish society.

Digital sovereignty is not solely a matter for the state. Every organization needs to know where its critical data resides, who controls the surrounding infrastructure, and what it means when that control is exercised by someone other than the organization itself.

5. The way forward

What has already left the app is lost. What leaves from this point forward is not.

Today, all organizations must be regarded as technology companies. Boards and executive leadership can no longer delegate this responsibility solely to a technical function. As organizational leaders, there must be an understanding of the business as a whole and how its components interrelate.

This report highlights a structural problem from two perspectives.

The first concerns responsibility for the applications the organization develops and publishes. The majority of the apps reviewed transmit personal data to third parties without a legal basis. 95 percent of the data leaving these apps is sent to companies outside Europe.

The second concerns the operational risk associated with employees' app usage—on corporate devices and on private devices used for work. The same information leaked by apps can be purchased from data brokers and used to map the organization. In addition, documented weaknesses in apps mean that business-critical data can be exposed.

The situation is serious. But it is addressable.

By reviewing mobile applications and making balanced, informed decisions, you do more than comply with legal requirements. You take a position on where the boundary of the organization's digital exposure should be. **Regulatory compliance, information security, and digital sovereignty are not three separate issues. They overlap.**

Three steps to control

Step 1: Gain visibility

Determine how applications behave in real-world use, in the hands of an actual user. An independent dynamic assessment reveals which external parties the app contacts, which SDKs it contains, which access permissions it requests, and whether the consent mechanism functions as stated. This applies to all applications within the organization—both those you publish and those used by employees on corporate mobile devices.

Step 2: Make decisions

For the applications you publish, there are three fundamental questions that must be addressed based on the assessment.

1. External service providers. Which ones do you want to retain, and why? Which are necessary for the app to fulfill its purpose? Which are not? Ensure a legal basis, data processing agreements, and, where transfers occur outside the EU/EEA, appropriate impact assessments.

2. Access permissions. Does the app need access to location data, the camera, contacts, or health data to perform its function? Any access that cannot be justified should be removed.

3. Consent mechanism. If the app transmits data to third parties, informed consent must be obtained. The solution must allow users to decline without negative consequences and must always act on the user's choice.

For the applications carried by employees, the decisions are different.ra.

1. What risks are associated with the nature of the organization's operations?
2. Which apps are business-critical and approved?
3. Should private devices be permitted for work, and if so, under what conditions?
4. Do certain roles require special handling?

Step 3: Act and Verify

Once changes have been implemented, it must be ensured that risk has in fact been reduced. This is done by repeating steps 1 and 2.

If you publish your own apps, each new version must be tested. An app that was compliant at launch is not necessarily compliant six months later. Continuous oversight is required to ensure that SDK providers do not introduce changes that conflict with your decisions.

Who does what in your organization

Responsibility for an app's data protection and information security is typically distributed across multiple functions.

Compliance and the DPO (Data Protection Officer) are familiar with the legal requirements, but lack technical evidence of what the app actually does. The CISO (Chief Information Security Officer) understands the infrastructure surrounding mobile devices, but lacks visibility into what takes place within it. IT and development may have built the app, but do not own the compliance issue or the risk assessment.

An independent technical assessment resolves this. All three functions are provided with a shared, evidence-based foundation on which to act. Without it, the issue becomes stuck between departments. With it, progress becomes possible.

ONE EVIDENCE BASE, MULTIPLE FRAMEWORKS

The technical assessment of what an app actually does is not solely a GDPR exercise. The same body of evidence addresses requirements across multiple regulatory frameworks simultaneously.

- GDPR requires documented data flows, a legal basis for processing, and an up-to-date privacy policy.
- ePrivacy requires a legal basis for accessing the user's device and communications data.
- NIS2 requires risk management across the entire supply chain, and an SDK constitutes a subcontractor within the product.
- ISO 27001 requires documentation of information assets and control over external service providers.
- SOC 2 requires demonstrable control over who has access to data and how it is protected.
- One assessment — not five separate projects.

More efficient management and a stronger competitive position

Each unnecessary third-party relationship that is removed represents one less data processing agreement to manage, one fewer potential impact assessment to conduct, and one less source of legal exposure to address. This not only reduces risk—it also lowers the cost of governance.
But this is about more than risk reduction. Organizations that can demonstrate control over their digital flows, and clearly document what their applications do and do not do, gain a competitive advantage—in their engagement with supervisory authorities, in procurement processes, and in dialogue with customers and partners who demand digital credibility.

Taking control of what your applications do is not only a matter of compliance. It is a business issue—and an information security issue.

You do not have to do everything yourself

The steps outlined above can be carried out by an organization independently. This requires technical expertise to conduct the dynamic assessment, legal expertise to interpret the results, and ongoing capacity to repeat the process with each new release.

It can also be managed as a service: independent assessment, legal interpretation, technical remediation within the app, followed by a validation assessment to confirm that the measures taken have had the intended effect. The internal team retains ownership of the decisions, but does not need to carry the full execution.

For organizations that view mobile applications as part of a broader effort related to digital infrastructure and risk management, there is an opportunity to integrate this assessment with ongoing work on the supply chain, cloud infrastructure, and information security. Visibility into what actually occurs is a prerequisite for making the right priorities and allocating resources where they deliver the greatest impact.

Om Peak Privacy och Shibuya

PEAK PRIVACY

Platform for autonomous app compliance and vulnerability analysis. Used by the Danish Agency for Digital Government. We make it easy for organizations to demonstrate evidence-based compliance to supervisory authorities, boards, auditors, and customers.

Vibeke Specht · Medgrundare
vibeke@peakprivacy.eu
peakprivacy.eu

SHIBUYA

Swedish cloud provider since 1964. A family-owned technology company delivering mission-critical IT from Swedish data centers. Local support and monitoring around the clock, under Swedish and European jurisdiction.

Andreas Lundgren · Compliance & Security
andreas.lundgren@shibuya.se
shibuya.se