Privacy and Security - The Friendship That Needs a Coffee Date

Executive Summary

Privacy and cybersecurity have been handled as separate disciplines, one governed by lawyers and compliance officers such as the Data Protection Officer (DPO) and the other by Chief Information Security Officers (CISOs) and technical experts. However, while the main perspective of each is different, they are both part of the information and data ecosystem adding to an overall digital security landscape. They are two sides of the same coin, hence, a strict separation is not ideal. Organizations now face increasingly complex digital threats, stricter digital regulations and a growing number of digital entry points. This is especially important for companies with mobile applications, due to their nature of being black boxes. Mobile applications' privacy and cybersecurity is overlooked, yet it is a cause for critical vulnerabilities.

As digital compliance frameworks such as NIS 2, GDPR, ePrivacy, ISO 27001, SOC 2 and NIST evolve toward an integrated risk-based approach, the message is clear: privacy and cybersecurity practices should follow this path together. Because in one way or another, both domains aim to protect the same asset, data. The difference is in the perspective. A strong privacy framework strengthens cybersecurity posture through better data governance, while robust cybersecurity controls protect privacy by preventing breaches, data leaks and data misuse.

This paper explores how privacy and cybersecurity complement each other to build trust and strengthen the overall digital security posture of organizations. It also highlights how Peak Privacy enables this collaboration by bridging a communication gap between DPOs, CISOs and IT professionals as well as between governance and technical execution within mobile ecosystems where most visibility and auditing mechanism fail.

The Changing Digital Landscape

Digital ecosystems have become encompassing and powerful. Data-driven business models are dominant and so are the new threats and risks they bring. This is also reflected by new digital regulations with an ever expanding scope and requirements regarding data. The, by now well known, General Data Protection Regulation (GDPR) aims to protect personal data and limit privacy-violating data processing within the European Union. According to the GDPR Enforcement Tracker, since the regulation was put into action in 2018 there has been a total of EUR 7.5 billion in fines recorded to this date (October, 2025)[1]. This is a clear indication of the extent of data-related unlawful behavior.

Similarly, the new NIS 2 Directive aims to protect data by applying confidentiality and integrity requirements. Non-compliance with the compulsory requirement can mean extensive financial damage for companies with fines of up to €10 million or 2% of companies' total annual global turnover for essential entities, and up to €7 million or 1.4% of their total annual global turnover for important entities. Moreover, the scope of NIS 2, compared to the previous NIS has been extended to industries with high social responsibility and increased digitalization. One of NIS 2's most discussed requirements is the supply chain security requirement. It means that companies under the scope of NIS 2 are directly responsible for the cybersecurity of their supply chain. This can impose cybersecurity requirements on companies outside of the original scope of the directive[2].

Reports from ENISA (European Union Agency for Cybersecurity) constantly emphasizes the importance of implementing digital protection tools aiming to protect organizational and user data. The agency adds that this can be best achieved by analyzing privacy-by-design principles for new electronic products and services. The agency suggests that technical measures and safeguards must be implemented at the earliest stages of data processing operations implying that security professionals need more information on actual processing activities to implement efficient and targeted cybersecurity tools and organizational measures[3].

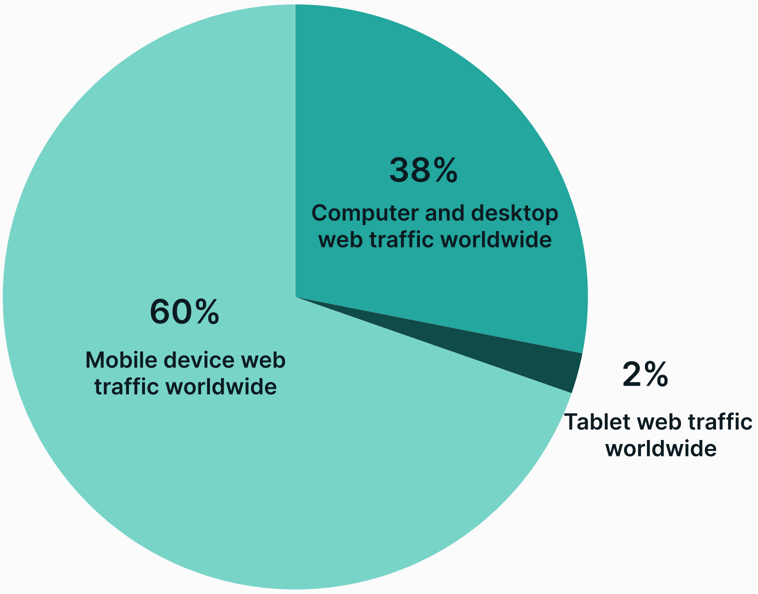
This reinforces a key point: privacy and cybersecurity are no longer parallel disciplines, they are interdependent pillars of digital trust.

The Mobile Blind Spot

With the evolution of technology, new techniques of data sharing, data processing and data storing emerged. One of these platforms was mobile devices and mobile applications[3]. While web environments are more focused on and easier to control by now, mobile applications remain the Achilles' heel for many corporations and organizations. App code bases often contain multiple third-party components, called Software Development Kits (SDKs), alias external code particles that collect, transmit, and process user data. Each update can introduce new SDKs or change vendor behaviors, often without the organization being aware. This is not a theoretical concern, it is real life.

Recent cases, such as the Gravy Analytics data brokerage incident, revealed how mobile data, in this case location data, was collected and shared without user consent and without the knowledge of application owners. The brokerage broadly sold and redistributed the location data to unknown parties. This unlawful action culminated when Gravy Analytics' network suffered a data breach, unveiling tens of millions of location data points tracking where people had been, lived, worked, or travelled[4].

Mobile applications make up more than 60 percent of the internet traffic today[5]. Unlike websites, mobile apps operate as black boxes bringing about new threats and new challenges. It is almost impossible for non-technical professionals to understand what data is collected, where it is sent and whether it complies with GDPR and security and privacy standards like ISO 27001 or SOC 2. Especially without a specialized tool.



Top mobile risks in 2024 included inadequate supply chain security, inadequate privacy controls, insecure data storage and insufficient cryptography[6]. These risks can be directly added to an organization's risk registers under ISO 27001, SOC 2 and even under the new NIS 2 Directive for companies within the scope.

- **Inadequate Supply Chain Security**: a supply chain vulnerability for mobile apps mainly happens because of the lack of secure coding practices and insufficient testing. Moreover, weaknesses in third-party software components, like unknown SDKs, and insufficient security controls for data can expose sensitive data to unauthorized parties[6].

- **Inadequate Privacy Controls**: most apps process some kind of Personally Identifiable Information (PII). However, many of them collect and process even more than they need[6]. Because of this, the risk of privacy violations increases and business operations do not comply with information security and privacy controls of industry standards as well as privacy laws.

- **Insecure Data Storage**: threat agents exploit vulnerabilities due to insecure data storage. This can include weak encryption practices, insufficient data protection and data storage mechanism. Moreover, the lack of secure data transmission protocols leave data vulnerable between the mobile app and external servers[6].

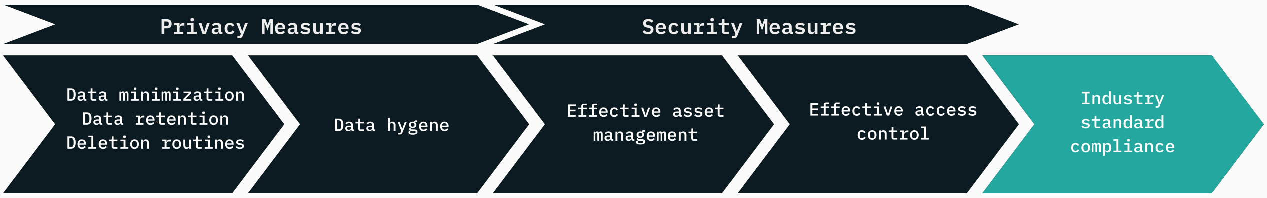
Peak Privacy scans mobile applications to detect data transmissions, revealing the "hidden data flows" that traditional audits miss. This visibility supports both privacy and security compliance by mapping data transfers, third-party dependencies, and potential vulnerabilities.

Why Privacy and Security Must Work Together

Modern cyber threats target data as much as infrastructure[3,7]. Although privacy and cybersecurity come from different traditions, they reinforce one another through shared practices.

Data Governance

A clear example of this interplay appears in how both domains manage data. Strong privacy governance encourages data minimization, defined retention periods, and deletion routines. These practices reduce the amount of unmanaged data stored across systems, which decreases the potential impact of a data breach. Security frameworks depend on exactly this kind of data hygiene to maintain effective asset management and access control[8]. In other words, **the more disciplined the organization is about what data it collects and keeps, the smaller the attack surface becomes**.



Vulnerability Handling

Vulnerability handling is another area where privacy and security intersect. Privacy requires organizations to prevent personal data misuse and unintentional exposure, while security focuses on infrastructure gaps and remediation to prevent exploitation. If privacy teams identify high-risk personal data assets, security can prioritize these systems in vulnerability management workflows[9]. **This alignment not only reduces real-world exposure but also supports compliance with vulnerability handling obligations under GDPR and NIS 2.**

Audit & Documentation

Both privacy and security depend on accurate documentation. Privacy frameworks require records of processing activities (RoPA), Data Processing Impact Assessments (DPIAs) and legal justification for data usage. Security frameworks require incident logs, risk registers and operational resilience documentation[7]. **When documentation is shared and structured cohesively, organizations reduce audit burden and demonstrate accountability more efficiently.**

Supply Chain & Third Parties

The same alignment applies to managing external suppliers and third-party technologies. As a risk assessment practice, privacy teams conduct Data Protection Impact Assessments (DPIAs) and evaluate whether processors handle personal data appropriately[3,10], while security teams assess vendor security posture and technical dependencies[2]. When these risk assessments inform one another, organizations gain both better transparency and stronger supply-chain control. If they were done in isolation, high-risk suppliers could slip through unnoticed simply because each side assumed the other was handling the evaluation.

In practice, this can also expose organizations to mobile app risks related to inadequate supply chain security. Attackers may exploit weaknesses within third-party dependencies, like vulnerable third-party SDKs and network requests. This scenario emphasizes the need for integrated privacy and security reviews from development through deployment[6].

For example, when a DPIA identifies risks in third-party data flows, the security team can apply technical controls, adjust configurations or change system architecture to mitigate those risks. Both sides benefit, but only when they are aligned and operating with the same visibility[3].

Supplier & Third-Party Vendor Assessment

Privacy POV	Security POV
• Data Protection Impact Assessment (DPIA) • Data processing practices • List of SDKs used in mobile apps	**Technical dependencies** • Multi-Factor Identification (MFA) • Single Sign-On (SSO) **Cybersecurity measures** • Secure development • Back-ups • Access Control Management • Continuous system monitoring for unusual data flow

Mitigating risk related to privacy and security are strongest when they feed into each other. This is the essence of the concept **trust-by-design**.

Trust-By-Design

Now more than ever, organizations must embed privacy and security measures throughout the development lifecycle rather than treating it as a separate compliance exercise. Among others, the implementation of secure coding practices, code review and testing throughout the apps' development lifecycle is recommended to mitigate vulnerabilities[6]. These measures are focused on risks and threats and their prevention and mitigation, contrary to a more reactive action. They build the trust to identify vulnerabilities within the systems.

Security-by-design emphasizes the importance of focusing on cybersecurity measures during the product development lifecycle to decrease the number of exploitable flaws, while **privacy-by-design** requires that personal data is protected throughout the entire lifecycle of data processing[8].

Trust-by-design, by fostering collaboration between security and privacy, creates a standardized system, one that makes it easier to adapt to new data-related legislation and also ensures transparency. But transparency is not just about visibility. Determining whether processes are functioning reliably requires clear, well-articulated insights into how they work. By embedding testing tools into these procedures, organizations can build a transparent, end-to-end trust system[11]. The identification of privacy related threats during application development can complement security engineering and security threats as well as increase accountability and provide documentation[7]. Here you can see how privacy and security assessments complement each other during the application development process and which information security requirements and processes can benefit from this collaboration:

Development Lifecycle Stages			
Design	Privacy-by-Design	Security-by-Design	Trust-by-Design
Development	Vendor Impact Assessment | App Settings	Supplier Security Assessment | Cybersecurity Tools	Shared Risk Assessment Practices
Deployment	Privacy Testing	Security Testing	Initial Vulnerability Scanning and Early Mitigation
Maintenance	Privacy Testing after each New Update	Incident Detection and Response	Continuous Adaptation
Decommissioning	Data Deletion	End-of-Life Procedures	Reports for Audit Purposes

Peak Privacy is uncovering privacy threats such as threats against the data subject rights and violations against data protection principles.

These threats should be monitored during the development process and applications should be tested for them before deployment or after each update release. The tool serves as a perfect complement for security threat monitoring since it uncovers non-compliant behavior of the application as well as supplier SDKs used to develop it. This threat modeling and threat handling plays into frameworks such as NIST, ISO 27001 and ENISA.

How Peak Privacy Supports the Trust-By-Design Model

Peak Privacy operationalizes trust-by-design within mobile environments. The service is designed to address the most pressing challenges in mobile data governance and digital risk management, especially when it comes to third-parties and regulatory compliance. Our solution enables faster compliance work, while facilitating a less siloed communication approach between privacy, security and IT professionals within an organization. The service supports:

- ***Data Flow Detection:*** Identifies unknown SDK transmissions and third-party endpoints by autonomously testing each application as a human user.
- ***Cross-Department Communication***: Translates technical behavior into regulatory meaning. The reports can serve to explain developers which technical elements are troublesome without the need for compliance professionals to learn deep technicalities.
- ***Risk Mitigation Support***: Peak Privacy enhances awareness and supports informed decision-making on development practices and supplier choices, reducing both privacy and security threats.
- ***Third-Party Risk Assessment***: Provides insights into new SDK suppliers and their data practices supporting the supply chain requirement under NIS 2.
- ***DPIA Support***: Identifies privacy risks after each app update, enabling remediation.
- ***Audit Evidence***: Documents how each app aligns to GDPR, NIS 2, ISO 27001 and SOC 2.

Peak Privacy does not replace internal expertise, it **enables collaboration** where visibility is currently impossible.

Reference List

[1] GDPR Enforcement Tracker by CMS.Law: https://www.enforcementtracker.com/

[2] NIS 2 Directive - EUR-Lex. (2022). EUR-Lex - 32022L2555 - EN - EUR-Lex. Europa.eu. https://eur-lex.europa.eu/eli/dir/2022/2555

[3] European Union Agency for Cybersecurity, ENISA (2022). Data Protection Engineering, From Theory to Practice https://www.enisa.europa.eu/publications/data-protection-engineering

[4] Whittaker, Z. (2025, January 13). A breach of Gravy Analytics' huge trove of location data threatens the privacy of millions. TechCrunch. https://techcrunch.com/2025/01/13/gravy-analytics-data-broker-breach-trove-of-location-data-threatens-privacy-millions/

[5] Bouchrika, I. (2025, November 7). Mobile vs Desktop Usage Statistics for 2025. Research.com. https://research.com/software/guides/mobile-vs-desktop-usage

[6] OWASP Mobile Top 10 | OWASP Foundation. (2024). https://owasp.org/www-project-mobile-top-10/

[7] LINDDUN. A Framework for Privacy Threat Modeling https://linddun.org/

[8] Folorunso, N. A., Wada, N. I., Samuel, N. B., & Mohammed, N. V. (2024). Security compliance and its implication for cybersecurity. World Journal of Advanced Research and Reviews, 24(1), 2105–2121. https://doi.org/10.30574/wjarr.2024.24.1.3170

[9] European Union Agency for Cybersecurity, ENISA (2022). Coordinated Vulnerability Disclosure Policies in the EU https://www.enisa.europa.eu/sites/default/files/publications/Coordinated%20Vulnerability%20Disclosure%20policies%20in%20the%20EU.pdf

[10] General Data Protection Regulation (GDPR) – EUR-Lex. (2016). EUR-Lex - 32016R0679 – EN – EUR-Lex. Europa.eu. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[11] Kumar, S., Jacobs, S., & Koehler, T. (2022). Trust by Design: Rethinking Technology risk: Enhancing technology risk management in agile environments to ensure auditable trust! In Compact Magazine.