ZOHO for Enterprise

5 years post-GDPR

How privacy is changing the security game

Security series, Q2 2023

Europe's groundbreaking privacy legislation has delivered lasting changes, bringing security and data privacy to the forefront of operations and design.

Five years into GDPR, as more and **more US states** implement their own versions of privacy regulations,[1] compliance is becoming an ever bigger line-item in every budget. Spurred by social pressures and legislative measures, organizations are undertaking changes in how they capture, use, and store data.

Companies that rely on data to generate revenue must adapt quickly if they hope to reach consumers without third-party cookies, tracking, and other surveillance practices common in the digital age. This adaptation comes at a cost; in the EU, businesses creating compliant systems saw an average 2.2% dip in sales and an 8.1% decline in profit.[2] Of course, when compared to the cost of a data breach or service outage, these losses are negligible.

The mind-boggling fines paid by Big Tech for violations regularly grab headlines: Meta's $405M penalty in 2022, or the $877M Amazon paid in 2021.[3] But GDPR has actually meaningfully impacted how business is done by companies that aren't racking up violations. Though eye-popping fines garner most of the press attention, the bigger story is how GDPR is transforming organizational operations, customer communication and product development.

Biggest GDPR fines to date:

- **$877M** Amazon (2021)
- **$405M** Meta (2022)
- **$400M** Google (2022)
- **$400M** Meta (2023)
- **$267M** WhatsApp (2021)

[Data Privacy Manager, 2023]

[1] Reuters, 2023 | [2] Tech Monitor, 2022

[3] EQS Group, 2023

Privacy by Design

While most organizations live in a reactive pose with regard to data privacy, privacy-first organizations are already defaulting to the standard of Privacy by Design (PBD) even when not legally mandated to do so. These privacy-first positions demonstrate a far deeper respect for user's rights, compared to the surreptitious surveillance systems that have made AdWords Google's most profitable product. There are many approaches to creating GDPR adherence, but they all live under the development and design standard of Privacy by Design.

And though GDPR speaks specifically to consumer rights, these can only be fulfilled through the implementation of new processes, roles and policies prioritizing the information security of every data subject. Security protocols like access management and encryption can't be relegated to a single line on the pre-release checklist. In this way, GDPR is not adding excess costs or bottlenecks, but simply mandating security considerations earlier in the development process.

No one should have to "opt-in" for privacy. That why Zoho applies GDPR-level data policies to every single account by default, rather than by request. And as the requirements for safeguarding information evolve, we will apply the most stringent policy to users worldwide. Legal mandates shouldn't govern these decisions; respect for user privacy should.

PBD in action

Privacy by Design is a philosophy encompassing 7 principles of security, transparency, ethics, and respect:

1. Prevention rather than remediation

2. Privacy as the default setting

3. Privacy embedded into design

4. Full functionality

5. End-to-end security

6. Visibility and transparency

7. Respect for user privacy

1. Prevention rather than remediation

Data security requires a proactive approach. Prevention is the goal, and privacy measures can't be strictly remedial.

Many organizations focus on preventing the threat from outside: the malicious data breaches that lead to compromised or lost data. But the far more likely GDPR violation is often overlooked: accidental data ingestion. Privacy-minded organizations need to be poised to identify and intervene to prevent inadvertent (or excess) collection of data. In cases where leakage has occurred, it is essential that teams develop procedures for deleting data from any systems that might have been fed information.

Ongoing audits aimed at minimizing data collection are an important way to reduce exposure risk. Fine-tuning input controls by rewriting questions to which users enter data can also reduce unnecessary information capture. Every product or micro-service can have its own clearly defined scope limiting the instances when data can be collected, and how the collected data can be used. Regular audits and documentation keep developers and system architects attuned to the ongoing security measures needed to meet user privacy obligations.

2. Privacy as the default

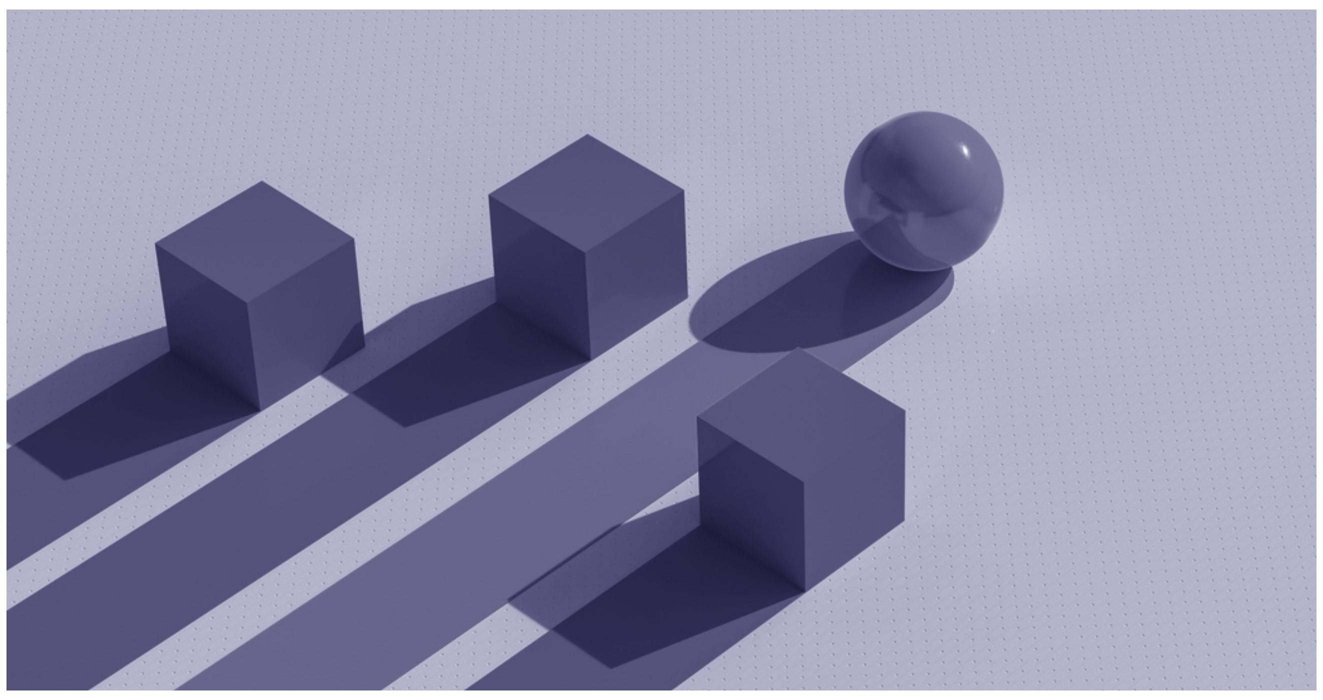
Privacy by design demands privacy as the default. This means that all processes and technologies are deployed with the starting point providing maximum user privacy. In consumer communications, this looks like leaving all consent boxes unchecked; joining a mailing list requires a multi-step opt-in from the user. In short, data is only captured after clear, active consent has been obtained.

3. Privacy embedded into design

Privacy is often a direct result of security choices. Organizations on the leading edge of GDPR have found ways to fully integrate privacy and security checks into their IT architecture and the processes it drives. In practice, this takes many forms: securing data across every stage of the lifecycle (at creation, in transit, and at rest); clearly establishing data retention and deletion policies; anonymizing log-ins given to support teams, or obfuscating private information through the UI; and enforcing the same standard of validation rules for all user operations, kept consistent by security guardrails within each element of the tech stack.

4. Full functionality

Of all the principles, this is the most self-explanatory: a user should never need to sacrifice privacy in service of making a product work, or "work better." In other words, this ensures that total functionality and total privacy are not mutually exclusive.



In a design culture driven by PBD, these two needs go hand in hand.

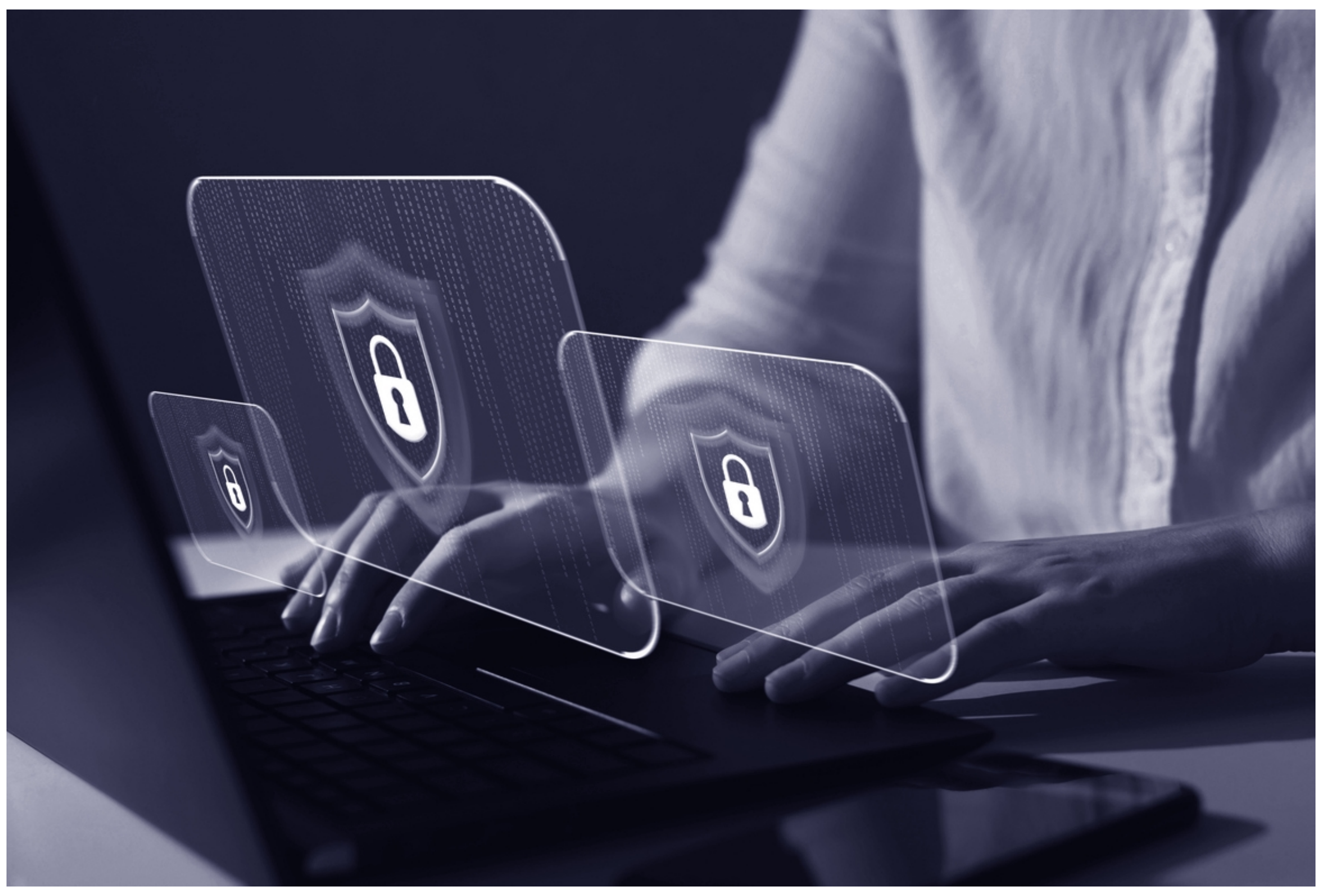
5. End-to-end security

Privacy is the result of end-to-end security; data has to be protected at every point in the lifecycle. But this practice can move beyond what's established in the tech infrastructure to include audits of usage, components, and micro-services.

All third-party API calls and other micro-services should undergo validation and authorization before being implemented, complete with detailed processing contracts limiting the exchange of data. Because outdated code offers malicious actors an easy, and often undetectable, way into operating systems, audits should also review static code to remove or update outdated modules. Regular audits and penetration testing are the easiest and cheapest ways to ensure data security and user privacy throughout the data lifecycle.

6. Visibility and transparency

The spirit (as well as the letter) of privacy law is marked by transparency and visibility. This means an ongoing openness to auditing and verification of systems and processes, and clear communication about how data is processed, used and stored. Transparency also means clearly established data usage policies that are visible to the public, alongside equally detailed policies for the employees designing products and processes.



This also means not gating basic website functionality behind “cookie walls” or requiring users to submit to surveillance; cookie banners requesting consent should give “accept” and “reject” equal prominence. An ethical design is one where users are pushed to act in their own best interests, not in those of the data collector. Rather than requiring users to navigate a maze of legalese and jargon, design should help users locate, access and understand their available privacy options without obscuring them in fine print.

7. Respect for user privacy

Above all else, GDPR requires ethically engaging with customers about when and why their data is being collected. This means only collecting data through active (and reaffirmed as needed) consent, and with clear and humane policies detailing how long data is stored and secured. Fundamentally, it requires doing everything to minimize chances for unsolicited data capture, as well as having the security systems in place to ensure that private data is never made public.

> ***More than 18,000 Data Protection Officers were hired in the first year after GDPR was passed.***
>
> [IAPP, 2019]

Internally, requests to change or increase data collection processes should be subjected to the same scrutiny, discussion, and documentation as the initial request, with approval coming from all relevant stakeholders as well as the DPO (in cases of major change).

The introduction of the DPO

The most visible staffing change in organizations looking to be GDPR compliant is the appointment of a Data Protection Officer (DPO). More than 18,000 were hired in 2018 alone.[4] The DPO, whether an internal hire or an external team of consultants, is tasked with ensuring that any PII (Personally Identifiable Information) and attendant metadata are only used in ways that are legally compliant and adhere to all promises made to data subjects. At Meta, more than 1,000 employees were brought on to ensure compliance with the privacy regulations.[5]

Of course, DPOs are only successful as much as they are empowered to act. GDPR demands that privacy live at the heart of every decision, no longer left to individual teams or piecemeal solutions. As Andrew David Baghyam, Zoho's DPO, notes, "The only way to ensure we can do our jobs is to know we will be heard. That's why we report directly to our CEO, rather than being dependent on product teams to decide the validity of any concerns. This informs our privacy-forward thinking, evident in everything from our marketing practices to our data migration processes."

More changes ahead

State and federal legislative bodies in the US are starting to prioritize data privacy and security in long overdue ways. As consumer awareness about data privacy continues to grow, employees (and organizations) of every stripe will have to embrace a culture in which privacy is paramount; when an organization becomes known for privacy failures, customers quickly jump ship.[6]

A privacy-first stance that's gaining popularity is expanding from encryption-at-rest (EAR) to privacy-enhancing computation (PEC) options that protect data while it is in use. Gartner predicts that more than 60% of large organizations will be employing at least one PEC technique by 2025.[7]

[4] IAPP, 2019 | [5] CEPR, 2022

[6] YouGov, 2023 | [7] Gartner, 2022

> “Privacy means fostering an internal culture where customer data, its value, and the dynamic nature of emergent threats, is at the front and center of conversations. This is the key distinction between organizations embracing the new reality versus those always playing catch-up.”
>
> **- Andrew David Baghyam, DPO at Zoho**

Setting up the education and processes to forefront privacy carries expenses with it, but the security infrastructure needed to fulfill GDPR obligations is the same infrastructure that will mitigate fault if a breach does occur. For organizations that thrive on customer data, GDPR is giving them the push they need to protect themselves in ways they should already be doing.

Why Zoho for Enterprise?

Proven software, customer commitment, tremendous value.

Scalability & Reliability

Zoho for Enterprise reduces the cost of infrastructure, unifies existing apps, and solves complex business problems for increased enterprise fitness, resilience, and scalability.

Customization & Extensibility

Through granular customizations and powerful in-house developer platforms, Zoho lets you orchestrate workflows, streamline data management, and deploy world-class solutions at scale.

Security & Privacy

From owning our own data centers to GDPR compliance features, Zoho enables enterprise organizations to focus on core business priorities, rather than data management.

Enterprise Services

From data migration to consultation and implementation, our team is armed with the in-depth product knowledge and industry expertise to meet your unique technical requirements.

Are you ready to transform your organization?

We're here to help. Have a 15-minute, no-obligation call with one of our **Business Architects** to get all your questions answered.

Find us at **zoho.com/enterprise.** | ZOHO for **Enterprise**