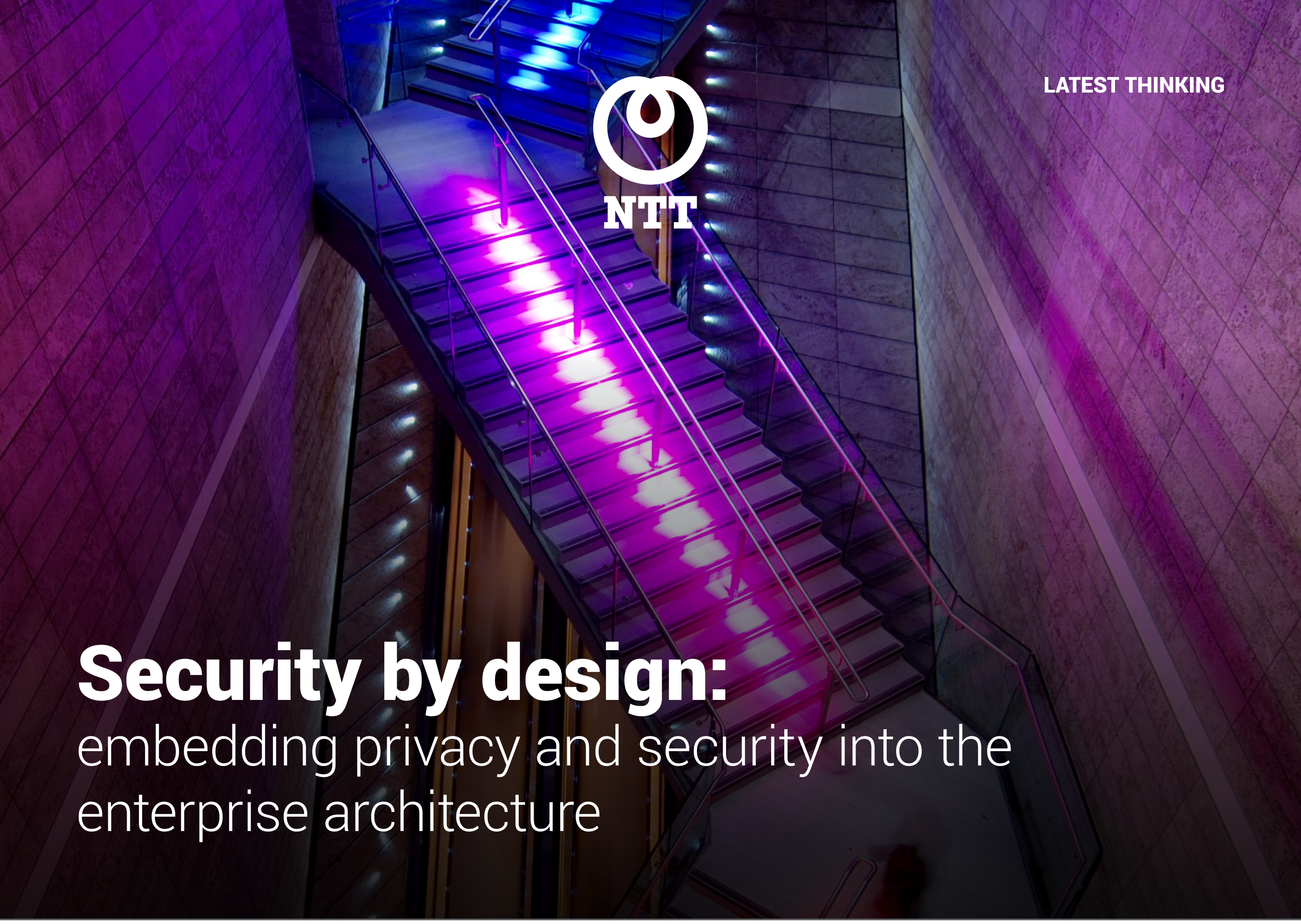


Security by design:
embedding privacy and security into the enterprise architecture

Steve Jobs once said, 'Design is a funny word. Some people think design means just how something looks. But of course, if you dig deeper, it's how it really works.'

Designing and delivering something that works is not just important in consumer products: it should also underpin every aspect of enterprise security, including an organization's enterprise security architecture (ESA). We all know what happens when security puts barriers in the way of people doing their jobs, but a well-designed ESA will reflect the strategic goals of the organization and be flexible and scalable enough to support new business ventures, technology, processes and people. If an ESA is carefully designed to work the way the organization does, it will also facilitate the relevant regulatory and legal requirements 'by design' – particularly when integrating security operations and governance with respect to data security and confidentiality.

Embedding security into the fabric of an organization, and every aspect of the way it works, is also key to successfully demonstrating compliance with the General Data Protection Regulation (GDPR). GDPR's guiding principle is privacy by design. Although privacy by design and privacy by default were originally introduced by the Canadian Privacy Commissioner of Ontario as far back as the 1990s, these concepts have been embraced by regulators around the globe as the foundations for privacy protection.

GDPR – design over fine

Putting privacy by design and privacy by default at the heart of GDPR demonstrates that despite the noise surrounding penalties for non-compliance, regulators don't want to rely on fines to change the way organizations treat personal identifiable data. With GDPR and other data protection laws, legislators around the globe seek a much wider transformation of enterprise culture. They understand that, however high the penalties, regulation by itself is not enough – particularly as many organizations operate a tick box approach to compliance and/or audit. GDPR recognizes that the only way to protect privacy in the digital age is to make data protection a fundamental component, not only in the design and maintenance of information systems, but in every aspect of business culture and how organizations touch and use personal data.

GDPR Article 25 (data protection by design and by default) codifies both the concepts of privacy by design and privacy by default. Under this article, data controllers and processors are required to implement the right technical and organizational control measures – not only when data is being processed, but when designing each of the data lifecycle stages: create, store, use, share, archive and destroy, by applying privacy protection from the outset. An example of this is the use of pseudonymization of personally identifiable information during different lifecycle stages.

The data controller must also ensure that, by default, only personal data which is necessary for each specific processing purpose is actually processed. In particular, this means ensuring that personal data is not automatically made available to third parties without an individual's consent. A practical example of this is that if you were creating a social media profile, the privacy settings should, by default, be set on the most privacy- friendly setting. Setting up profiles to be public by default will no longer be acceptable under the GDPR.

ESA – making privacy work, by design

For enterprise security architecture practitioners, the principle of privacy by design is nothing new. In many organizations, the function of ESA is not embedded into enterprise architecture; as such, security is often an afterthought, especially in the case of functions that process personal information on a regular basis such as marketing, HR, and finance. In our experience, the increase in brand- impacting cyber events, together with GDPR and other compliance drivers are reigniting the need for ESA practitioner support in projects and programs, as organizations seek to align their operations against the inherent security risks of our second industrial revolution. Enterprise security architects have the skills and business understanding to help those outside traditional security and governance roles to design and apply privacy by design and default principles. Enterprise security architects have a holistic view of the business and its objectives, so are able to advise on wider risk management strategies. Their job is to provide a security architecture that enables the business to meet its goals securely, not stop it in its tracks. A closer look at the principles of security by design demonstrates the synergy with ESA.

The seven principles of privacy by design

Rather than bolt on data security at the end of a project or just ignore it altogether, organizations that take a privacy by design approach will consider privacy and data protection compliance from the start when building new systems, considering sharing data with third parties, or using data for new purposes. The organizations that take this approach will see trust, brand reputation and commercial benefits very much in line with those delivered by a well- designed ESA such as:

- reduced risk in failure to meet data protection compliance
- increased awareness of privacy and data protection culturally within the organization
- early identification of potential privacy risks – reducing the time and money to remediate issues

So let's look at the seven principles of privacy by design:

1. proactive not reactive
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

Of all these valuable principles, if we had to pick two that will make the most impact on GDPR compliance and best practice security they would be 'privacy embedded into design' and 'end-to-end security'. Both of these points reinforce the need for strong security controls at every stage of the data lifecycle; from before data is collected, right the way through to when it is destroyed.

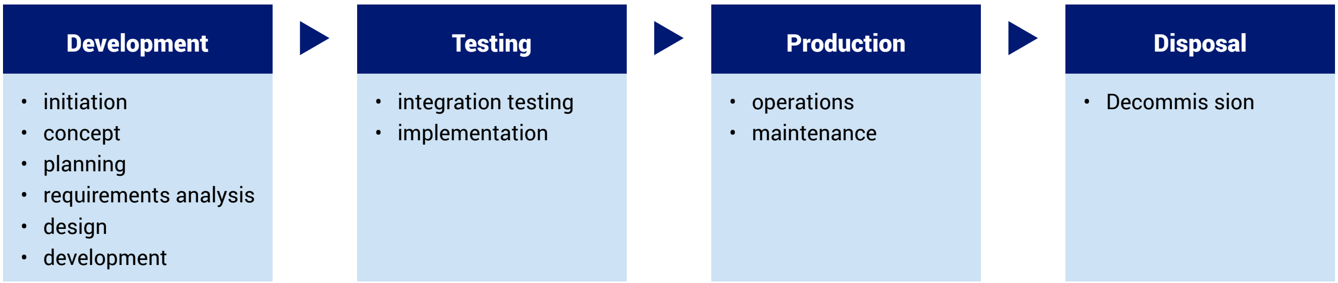
Managing this lifecycle in a way that works for every function in an organization has often proved difficult with the guardians of security and privacy gaining an undeserved reputation for slowing projects down or increasing the costs. The age-old business tension of risk and reward can either result in roadblocks following failed security risk or policy evaluation or worse – with business functions circumventing security controls, blasting through into the unknown and taking on risks that they do not fully understand or even consider.

Solving these issues is much less about technology and more about the culture, behaviour and understanding of data protection risk, and this is where we return to the skills of the enterprise security architect.

Our enterprise security architects are helping to challenge and change cultures and behaviours regarding new data protection regulations in practical ways. Looking at GDPR and directives like Network and Information Security (NIS) and how these align with existing regulations across in other regions –

When using this model, we encourage organizations to ask the following questions:

- Is privacy by design applied at every SDLC phase?
- Are risks defined, measured and managed?
- Are risks aligned with the right control layers, are these correctly applied and effective?
- Is there an effective ESA and governance to support enablement of policies, standards and processes?



Development
- initiation
- concept
- planning
- requirements analysis
- design
- development

Testing
- integration testing
- implementation

Production
- operations
- maintenance

Disposal
- Decommis sion

Figure 1 Privacy by design – tuning SDLC model

such as Privacy Shield in the US, Act on the Protection of Personal Information (APPI) in Japan or the Protection of Personal Information (POPI) in South Africa – our experts translate client-operated models like the Software Development Life Cycle (SDLC, Figure 1) linking the application of security controls and taxonomy. Tuning this familiar approach to consider (or perhaps encapsulate) privacy by design can help an organization focus on GDPR good practices and ensure that data protection and security are applied, by design, end-to-end across the enterprise.

Transforming compliance – more business understanding, less box ticking

If new regulations and directives such as GDPR and NIS Directive are to be successful in their aspiration to change cultures and implement enterprise privacy, data protection must emerge as an integral element of how a business works. Historically, some Governance, Risk and Compliance audit teams have contributed to their less than glowing reputation, by applying controls or standard industry templates and frameworks that are not in tune with the enterprise strategy, organizational objectives or Key Success Factors (KSFs).

And so for many business functions, there appears to be little or no understanding or context to their decision making. This disconnect not only leads to other business functions complaining of an apparent tick box approach to compliance that impacts operational and project delivery – but in our experience, also tends to result in increasing operational cost, poorly-defined enterprise security controls, inconsistent security practices and greater organizational complexity.

As we have established in this paper, in order to embed privacy and security into every part of the enterprise, business leaders and security leaders must align with a clearly-defined enterprise risk

Development	Benefits of a well-designed ESA
The Business	• **Visibility:** Proactive insight, essential for good corporate governance and executive decision making, helps mitigate or avoid security incidents, reducing impact on brand and bottom line. • **Strategy:** Business functions play a stronger part in strategy enablement, leading to improved operations and performance, and increased revenue through better utilization of security and business assets. • **Risk management:** Security by design is a business enabler – providing dynamic support for business challenges and change.
Central or Group Functions	• **Visibility:** Enterprise-wide insight into business unit and departmental Key Success Factors (KSFs). • **Strategy:** Enables development of an umbrella strategy, flexible enough to take into consideration the individual objectives and needs of the business units. • **Risk management:** Provides essential data to technology operations, supporting the evaluation of current 'known – unknowns', as well as 'unknown – unknowns'.
Departments and Business Units	• **Visibility:** Wider business gains clear understanding of the individual missions and key business constraints that may affect business units' go-to-market strategies. • **Risk management:** Focus on good practice to support, evaluate and mediate where objectives are at odds.
Investors / Shareholders	• **Visibility:** Evaluate current control assets and security programs to identify business value and ROI. • **Strategy:** Identify improvements to current control assets that will reduce operational costs, improving operating profit. • **Risk management:** Helps management identify and prioritize cyber risks, to mitigate or avoid incidents, reducing likelihood of brand and share price volatility.
Customers	• **Strategy:** Organization has effective corporate governance, with embedded 'security by design' culture that takes customer data and privacy seriously. • **Risk management:** Continuous service improvements in cybersecurity controls, processes, standards and responses help to grow brand trust.
Industry Stakeholders and Regulators	• **Strategy:** Organizations which invest in aspects such as customer data protection, cybersecurity practices and embedded 'security by design' culture, will be recognized for market-leading ambition. • **Risk management:** 'Security by design' strategy will be seen as commitment to taking regulations like GDPR and the NIS Directive seriously, business wide.

Figure 2: Organizations with a business-aligned, privacy-focused ESA function can see trust, brand reputation and commercial benefits including those listed above

strategy. Only when this is agreed can business analysts, enterprise architects and enterprise security architects work together on the evaluation and design of the right enterprise security architecture to support the enterprise data lifecycle, as well as addressing evolving business risks. An enterprise security architect will fully understand and have agreed with relevant executive stakeholders the organization's appetite for risk. Only with this intelligence front of mind can they support the design and alignment of the relevant policies, standards and processes, with the organization's goals and governance framework.

Privacy by design – the principle for ESA

Taking a step back from day-to-day security activities and technology maintenance can be difficult. The pressures of too many tasks and not enough resources can force many organizations to become reactive and tactical in their approach to security. But for organizations that want to regain control of how and where resources are invested for maximum impact, designing an enterprise security architecture not only highlights security complexity, but can provide end-to-end visibility of practices and controls and proactively bring privacy and risk management strategies in-line with the enterprise strategy and compliance.

For some forward-looking organizations, GDPR has become the catalyst for more than just the creation of another tick box compliance exercise. As those entrusted with driving GDPR projects, generally not IT professionals, seek to work with their security colleagues, the *privacy by design* concepts are igniting new conversations about enterprise risk management as a way to evaluate return on investment in people, processes and technology. Enterprise security architects, who are also more business professionals than deep technologists, can often form an effective bridge in these conversations about risk in terms of aspects such as: threat evaluation, return on investment (ROI), or annualized loss expectancy (ALE).

We have also seen the focus on GDPR result in resourcing discussions. Ensuring the appropriate levels of activity in areas such as alert management and incident response has led some organizations to use managed security services to provide the right flexible access to resource and response. Having a well-designed ESA also helps establish the context for third- party partners to be effectively deployed, briefed and managed to provide proactive intelligence as part of an organization's end-to-end security.

Privacy by design and default are undoubtedly principles shared by both GDPR and enterprise security architecture. But as GDPR will not be the last legislation organizations have to face, the sooner they enable a business-aligned ESA function, the better prepared they will be for whatever comes next.

Disclaimer: The work described in this thought leadership was performed while the company was known as NTT Security.

NTT