Column

Take it or leave it

Take it or leave it. It's a phrase you can expect when closing a deal on a flea market: no further bargaining, this is the best deal, accept it or not. Or maybe it reminds you of an old song written by The Rolling Stones. But you might not expect to hear it in the world of IT solutions. Yet, more often than not, it is the initial approach taken by SaaS providers, especially US-based vendors. Software as a Service: standard solutions used by hundreds of thousands of customers worldwide who need to accept its functionality as it is, or leave it be. That same approach is frequently applied by these vendors to their terms and conditions. With the argument that it is undoable to apply different terms to different customers in various regions. To some extent this makes sense. Offering a standard service comes with standard terms to keep the price competitive and to keep the different contracts manageable. Why would you even want to negotiate your own terms if all other clients are willing to sign up?

The reality, however, is challenging. In the evolving legal landscape in Europe the "take it or leave it" approach does not always match the legal and compliance requirements prescribed by legislators. This translates in more push-back by (potential) customers in Europe. Running a formal tender under EU law will further reduce the possibilities of vendors to make customers just accept the terms that are being offered.

We only have to take a look at developments in Europe in the domains of cyber and privacy to see that complying with all legislation is a daunting task. To name just a few: for a little over a year, the Digital Operations Resilience Act (DORA), with a focus on the financial sector, has been in effect – with a grace period to comply until January 2025. Financial institutions are by now quite familiar with (changing) legal requirements, but do not be mistaken: DORA is applicable to improve resilience in the entire supply chain in the sector, including IT service providers. Many organizations are already investing in strengthening their cyber resilience, for example by improving their existing Business Continuity Management and IT Continuity Management processes, amongst others driven by the Cyber Resilience Act (CRA) and Critical Entities Resilience Directive (CER). DORA aims to enforce institutions that had this topic on the backburner, in the right direction. It is based on the same principles as the EU's newly updated Network & Information Security directive (NIS2). NIS2 has an important difference, though, as it is a European Directive (which requires EU Member States to transpose the directive into their national law) and not a regulation (like DORA and the GDPR, which apply directly from the EU level to individual organizations and are binding for all organizations). EU Member States need to "translate" NIS2 into local legislation by the end of 2024, with the aim of it being in effect in early 2025. The fact that recently the responsible Minister in the Netherlands announced that the local translation has been delayed by at least a few months, is not a good sign that the Dutch government will meet the timeline in the Netherlands for the local translation of the NIS2. Especially for the organizations new in scope for NIS, this will mean a delay and a longer period of unclar-

Pieter de Meijer
Director
KPMG Cyber & Privacy

ity. Whatever the speed of national legislative processes, it is clear that resilience is a topic that is here to stay and that will impact the operations of most businesses and organizations with lasting effect. Take it or leave it.

In the realm of privacy, we saw a relative successful release and adoption of the GDPR almost six years ago. A strong point was the fact that this is a European regulation, directly applicable to all member states, and it further harmonized privacy requirements across Europe, more than its predecessor, the EU Data Protection Directive, did. The fear of significant fines increased the speed of adoption by many organizations. At the same time, we need to be realistic that enforcement is a local affair and penalties vary hugely per country. The national Data Protection Authority's capacity is often a limiting factor in following up on privacy incidents. And there is about to be a new kid on the block: the Artificial Intelligence (AI) Act. Again, this is a European legislation that directly applies to all member states. A difficult aspect is how the AI Act will be interpreted by local regulators or supervisory authorities, such as the Data Protection Authority. The Act defines a set of eight categories of high-risk AI systems to provide guidance on the requirements for different types of technologies and solutions, but the reality might prove that a lot of products will not (perfectly) fit these categorizations. This means it will require knowledge and experience to interpret in which category the AI solution fits. The AI Act does not only apply to the Big Tech companies. Deployers (the organizations rolling out the AI solution), distributors (the developers of the AI solution) and importers (the organizations importing and (re)selling the AI solution) all have their own requirements to comply with, although distributors and importers will have significantly more requirements to comply with than deployers. But when do you transition from a deployer to a distributor? Configuring, adjusting, and training the AI model will be seen as mutating the AI solution, elevating a deployer to a distributor. This "level up" is something that organizations need to monitor themselves; for example, it requires them to record the AI solution in the EU database. Whether you are a US-based company or not, the whole set-up of the AI Act will mean that if you want to deal with European customers (and citizens), you have to take it (or leave it).

What all this legislation has in common is the fact that the enforcement is, to put it mildly, challenging. The different laws have their own penalties, and in the case of DORA not even a formal one (although you could argue that the risk of losing a "license to operate" is a severe penalty in itself; and don't forget that the financial penalties from NIS2 also apply to critical financial sector entities). But the various laws also have different governmental organizations tasked with validating compliance with the legislation. In a number of cases, this role and this legitimate task are new to these organizations, and it is doubtful they will be ready in time to take up their mandate. The alternative of not being ready could have a devastating effect on the adoption of the various acts, making them just a hollow attempt to decrease relevant risks. Because this is key: this legislation is about reducing risks. All organizations should be mindful and apply a risk-based approach in the implementation of all these rules, despite the fact that some legislators would like to treat it as "principle-based". That might be easier said than done, but the alternative (taking a rule-based approach) is a severe effort to comply with many requirements that might not fit current processes and controls, leading to challenges to make the legal improvements "stick". And that brings us to the next level of maturity: test once, comply to many. Do not wait for the regulators or supervising authorities to validate your compliance with a specific legislation, but turn it around by implementing controls that can be tested once to show adherence to various frameworks at once. Avoid silos in the organization that focus only on a specific framework or requirement. This requires integrating all requirements and controls derived from different laws and regulations into one overarching framework that is fit for the purposes of *your* organization.

So, do we want to be known for our Dutch stubbornness, like the author of this column himself? If we don't want to take it, should we leave it? Gear up for the so-called Nexit? Whether you like it or not, The Netherlands is inseparable from Europe. For centuries we have been known as a country of trading, although not all Dutch trade can be considered righteous when viewed from our current ethical standards. We cannot treat our beloved nation as if we are a Gaulish village trying to resist the Roman Empire. If the history or the nature of these lowlands is not convincing enough, we only have to take a brief look at how the British people think about the Brexit nowadays. I'm sorry to disappoint those striving for full independence, but that's not going to happen. And if we can't leave it, we need to take it! Take these (legal) requirements and apply them for business benefit. And that same reasoning applies to US-based SaaS vendors: if you want to take the European market, deal with it. Or leave it.

Let's use the attention from politicians and regulators to improve our cyber and privacy processes, not just to comply, but to actually provide more trusted services and products to the market.