Regulators at the edge of tomorrow

by  **Pavol Adamec**, Executive Director KPMG in Slovakia

Over the years, digital systems became an integral part of our society. And the more our society becomes reliant on them, the more regulators have the digital world on their radar. The GDPR storm in 2018 was by far neither the first nor the last one in the digital area.

What matters

One can hardly find a regulatory area related to digital environment that would have higher influence on the society than GDPR. Despite that, no one should consider GDPR as a one-off topic. Many key aspects we can find in GDPR are the corner stones of trust in the digital era. Everybody involved in digital ecosystems should have those regulatory "moments that matter" on top of the agenda to survive.

Digital systems interact with natural persons, regardless of their role (employee, citizen, consumer). Protection of natural persons' rights in digital ecosystems will be of utmost interest to regulators as individuals typically have weaker roles in the ecosystem. Environments and the digital systems are complex and therefore difficult to predict – easy to break in many ways. Proper risk management of the digital systems' impacts is therefore a must. Digital systems run on data and with data – complete, correct, relevant data. The way the data management is done is therefore crucial for regulators to trust the results of the system. To trust the systems, one must trust the data are not disclosed or modified at will - cyber security is unavoidable in the regulatory shopping list. The digital world is a world of interconnected systems and services. Once you use external services, third party risk management starts to be your concern as you are accountable for the results regardless who contributes to them. To be trusted by regulators and business partners, transparency and oversight in every key aspect of your systems is required. And the last but not the least – even if you make everything right, things may go wrong. Proper incident readiness and response is what regulators expect you to master.

> ...even if you make everything right, things may go wrong.

It has nothing to do with me

Many companies think that digital regulation is not their issue. With the need to manage the risks of third parties, regulatory requirements for the digital environment cascade also to service providers. It does not have to be just processing of personal data by a third party that matters. In financial service, we see more of ecosystems of banks, with the funds and need to innovate, and fintechs and startups, with cool ideas but lack of funds to realize them. Many of these startups learned the hard way that to sell a cool idea to organizations possessing funds, you also must have them regulatory-ready to make the solution fly.

And it is not just secrets that need to be protected. EU NIS Directive pays attention to security of digital systems required for running services essential for the nation. Water supply, power, heat, pharmaceutical production, transportation, communication, oil and chemical industry, smart industry and many others. Frequently, it is not a leak of sensitive data that matters most. First, I care about having water, power, heat delivered and only than about keeping it secret how much I consumed. Tens of major companies in the country are coming in the regulatory focus for reason that used to be relevant only to bankers. "So how do you run your digital systems?" is a question these companies will be shortly asked by cyber security auditors.

Looking at the edge of the regulatory horizon

What has been a regulatory norm for banks for years is now becoming a norm for other sectors. Keeping an eye on trends in the regulations of the banking sector is a good way to be ready for what is to come.

> What has been a regulatory norm for banks for years is now becoming a norm for other sectors. Keeping an eye on trends in the regulations of the banking sector is a good way to be ready for what is to come.

While cyber security has been a dominant digital regulatory topic for banks for years, recent developments show that new focus areas start to appear. In July 2020, European Central Bank for the first time published key observations and conclusions stemming from its annual horizontal analysis of the IT Risk questionnaire. While cyber security is found to be a reasonably mature area, data quality management was reported as the weakest area. Besides that, the use and management of "end-of-life" systems for critical processes seemed particularly challenging for many institutions. The ECB also noted high outsourcing concentration risk, and many banks reported losses due to the unavailability of outsourced services.

The regulatory focus on data management is not driven just by reporting. Advanced data analytics is becoming a norm in the modern banking. While automation of processes has been common for years, automation of decision making promises much higher efficiency gains. So called "cognitive automation" means, simply said, lots of statistics. As humans, we understand discrete values. If I look at a group of people, I may conclude that the average person is female, dark-haired, blue-eyed. For a statistical system, the average person could be 0.7 female, 0.65 not-light-colored hair, 1.00 not having skirt (I forgot to mention it was winter-time). The meaning of statistical models' recommendations and the question of what data they were trained on to provide them – these are just a few of the concerns regarding advanced analytics.

The future is digital

If you think that regulators find technologies risky and do not like risks, you got it all wrong. In a blog post dated 8 May 2020, Pentti Hakkarainen, Member of the Supervisory Board of the ECB, commenting on the role of technology during the pandemic, made it clear: "Technology has kept the show on the road". The future is digital. Be digital or become extinct.