Strong authentication and minimum private data collection

The global cyberspace is anything but a uniform regime. Where from one corner of the cyberspace it may show up as strangely coherent and competent for global coverage, it carries along institutional settings and ideological preferences that may not be able or willing to merge together. Security of the global cyberspace, including, for example, the security of authentication services that are based on biometric identifiers, depends on **additional supportive institutions and interoperability frameworks**. Biometric information and processing of biometric identifiers as a component of the authentication process is an inherently sensitive process. Strong authentication is oftentimes equated to biometric authentication, such as fingerprint scanning as an additional component for endpoint security in mobile devices.

Security of strong authentication mechanisms relies on more than technical solutions and architectures. Most strong authentication mechanisms need to process sensitive information, biometric in the worst case, in order to achieve a sufficient level of strength. The level of security of those systems ultimately depends on the **level of security of the institutions its security is based on**. This does refer to more than just corporate security. Comprehensive cybersecurity environment also requires lawful and covert accesses and visibility, something that is usually out of the scope of the corporate environment, yet something they need to take into account. In the global context, the range of lawful and covert interceptors may be unknown and include also hostile entities. Companies therefore, need to reevaluate the data they choose to process and consider their responsibility towards their stakeholders' private and sensitive data, oftentimes minimize it in order to avoid/decrease risk.

Some companies may uphold a false or an outdated sense of trust and, thus, end up deploying identifiers and mechanisms that will ultimately expose their respective users to heavier risk of identity theft, industrial espionage and beyond. This can also become a business liability and a difficult risk to manage. Yet, modern data protection principles like GDPR put all the responsibility of reasonable protection on the data controller, which is the company running the services at the highest level in many cases.

We at Altipeak will ensure that we do our part, and that our applications do not collect or process any more private or sensitive data for the purposes of authentication other than what is necessary. Furthermore, we are glad to assist our clients to ensure that they do not expose their customers to further risks regarding privacy and protection of private data (e.g. biometric identifiers).