first™ strike

WHITE PAPER

1Strike.io platform

Entrepreneurs in the SME sector are required to comply with regulatory requirements, both the Regulation on the Protection of Personal Data (RODO) and other regulations related to the protection of personal data, information systems or cyber security, such as the Law on the National Cyber Security System (KSC).

The consequences of failing to comply with the law, including failing to implement adequate and effective measures for early detection of threats to systems, can be very negative, ranging from loss of image to the imposition of very high administrative fines. This is especially important given the growing cyber threats. In 2021. CERT Polska has registered 116,071 reports of cyberattacks, of which 29,483 were unique cyber security incidents. This number has increased by 182% from a year earlier, and this indicates an increasingly serious problem for businesses in this area.

The 1Strike tool can prove helpful and its functionalities crucial in ensuring compliance with the requirements of both Polish and European Union law, as well as ensuring the security of your organization. It allows you to constantly monitor threats and quickly respond to emerging security gaps.

It is incumbent on companies to apply security measures and respond to vulnerabilities as they occur, but continuous monitoring and reporting of threats and incidents is key. One-off actions are not effective, and according to regulators are not considered sufficient and can lead to very high fines. The reports generated by the 1Strike Tool can be successfully used as evidence of the continuous application of appropriate technical and organizational measures to ensure regulatory compliance. In addition, the application of recommendations to identified vulnerabilities increases the security level of the organization. An additional advantage is that no additional legal obligations, such as personal data processing entrustment agreements, are generated when using the Tool. In order for the 1Strike Tool to work properly, it is not necessary to transfer any data to third parties, which eliminates additional risks of data protection violations. The simplicity of the Tool provides convenience of use while maximizing the regulatory and security objectives of your organization.

RODO principle	Regulatory requirement	Compliance analysis 1Strike tools
Principle of legality, fairness and transparency	The controller must process data lawfully, fairly and transparently to the data subject. According to this principle, the controller must be able to inform the data subject in a clear and understandable manner about the processing process, risks, consequences, or entitlements.	The controller can immediately inform the data subject of the use of the 1Strike Tool in order to reduce the risk of a breach of the subject's personal data, which in the eyes of potential clients or customers or control authorities can have a positive impact. The use of the Tool also raises the level of awareness of potential risks, and thus the data controller has an easier way to prove legal compliance in terms of RODO or KSC.
Data minimization principle	It mandates that a minimum amount of data be collected by the controller, relevant, appropriate and limited to the purposes of processing, including in terms of time. It also refers to ensuring privacy by design.	The 1Strike tool does not interfere with or process personal data for any other purpose than to enhance the security of the organization, thus addressing the principle of minimization.
Privacy by Default	The controller is required to implement such technical and organizational measures so that, by default, only those data are processed that are necessary to achieve each of the processing purposes.	The 1Strike tool does not integrate into the data as a processor, does not have access to the data collected in the controller's systems, which eliminates additional data breach risks and raises the level of application of basic organizational and technical measures used in the organization.
Privacy by Design	The administrator is obliged to implement appropriate measures technical and organizational measures already at the stage of designing business solutions.	Implementation of the 1Strike Tool at the solution design stage business, to ensure security, will be in line with and expected by t h e RODO, especially for new technology solutions.
The principle of integrity and confidentiality	According to this principle, personal data should be processed w a manner ensuring data security, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage by means of appropriate technical or organizational measures.	It is from this principle, among others, that the need to regularly test, measure and evaluate the effectiveness of the measures technical and organizational designed ensure the security of processing. The 1Strike tool can be successfully recognized asone that implements this principle and helps the controller meet regulatory requirements.
Principle of accountability	One of the most important principles of RODO. Indicated in many places in the RODO. Each controller is responsible for compliance with data protection regulations and all rules and must be able to demonstrate compliance. It is the administrator's responsibility, in addition to applying appropriate measures, to document the actions taken and decisions on the choice of certain solutions to be able to demonstrate compliance with the processing with the RODO. The rule requires administrators to periodically review the effectiveness of these measures and update the assumptions and solutions used.	The 1Strike tool complies with the requirements to implement measures to ensure compliance with data protection regulations in connection with data processing operations, as well as to produce documentation that demonstrates what measures have been taken to ensure compliance with data protection regulations. The 1Strike tool keeps its database of cyber attacks (viruses) up-to-date, and each attack simulation operation at a given administrator is documented by generating a report at selected intervals. This shows ongoing control of processing security in the enterprise.