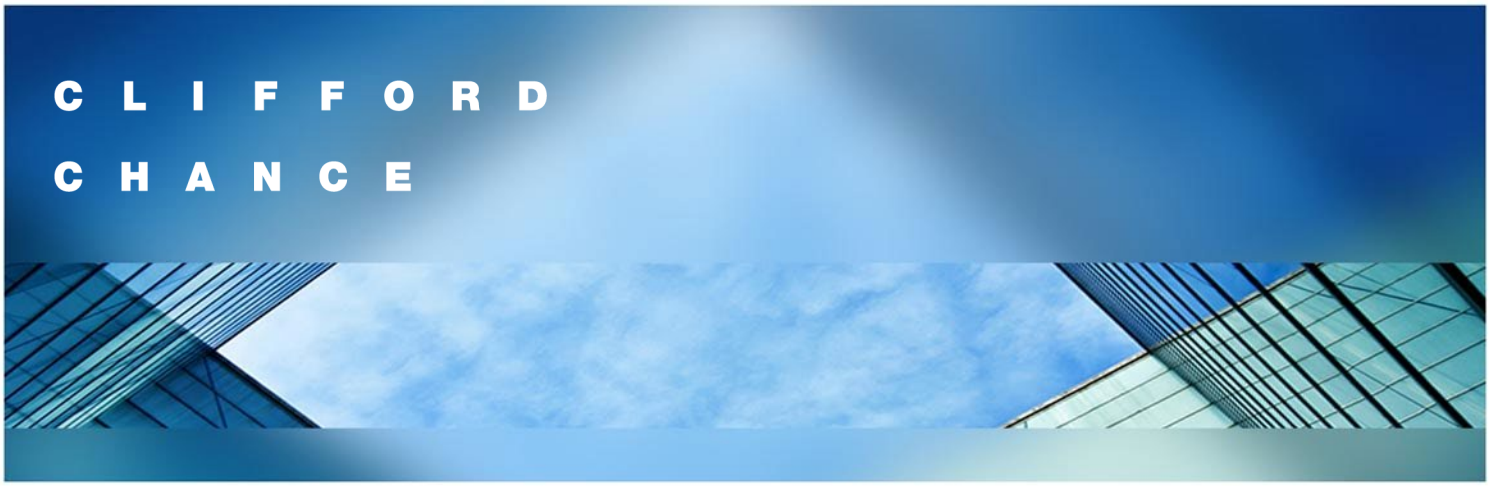

NEW POLISH ACT ON THE NATIONAL CYBERSECURITY CERTIFICATION SYSTEM AND ITS KEY ASSUMPTIONS

On 28 July the Act on the National Cybersecurity Certification System (the "**Act**"), which will enter into force 30 days after its publication, i.e. on 28 August 2025, was published in the Journal of Laws of the Republic of Poland. The main objective of the Act is to ensure the proper organisation of the cybersecurity certification system in the Republic of Poland by establishing appropriate procedures for issuing national and European certificates that will be recognised by all European Union Member States and defining the rules of supervision and control related to such certificates.

Compliance with the European cybersecurity certification framework

The introduction of the certification procedure results from the obligation to implement the provisions of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity ("ENISA")) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (the "Cybersecurity Act"). The Cybersecurity Act is the leading piece of legislation regulating the increase in the level of security of information and communications technology services (ICT) in the internal market of the European Union. Its assumptions include, inter alia, strengthening ENISA and ensuring the harmonious application of cybersecurity certification procedures in all Member States of the European Union.

Assumptions of the certification procedures

Regulation of the certification system is aimed at creating uniform security standards within the European Union and thus increasing the trust of consumers, customers and enterprises in products, services and ICT processes and preventing market fragmentation in the field of cybersecurity. According to the definition of "certification" in Article 2(3) of the Act, certification is to confirm compliance with the requirements set out in the European cybersecurity certification programme or the national cybersecurity certification scheme.

National cybersecurity certification schemes are a new legal institution that complements the Cybersecurity Act. It is a national certification programme, the preparation of which is to be the responsibility of the Minister of Digital Affairs.

Certification is to be a completely voluntary process that does not impose any obligations on market operators. Its scope will be specified on the basis of a contract concluded between the supplier and the compliance assessment body. In addition, national cybersecurity certification schemes also provide for the possibility of certification of both individuals and cybersecurity management systems.

Competent national authorities

The Cybersecurity Act requires EU Member States to establish a national cybersecurity certification authority for the purpose of market supervision and control of the correctness of the certification procedures. Article 4 of the Act appoints the Minister of Digital Affairs (the "Minister") as the competent cybersecurity certification authority. The Minister's tasks include, among other things, supervising the institutions comprising the national certification system, conducting inspections of such institutions, consenting to the issuance of European certificates with a "high" assurance level and examining complaints lodged against institutions assessing compliance within the scope of the activities carried out by these institutions under the European cybersecurity certification schemes.

An important role has also been assigned to the Polish Centre for Accreditation (the "PCA"), to which the legislator indicates specific information and supervisory obligations. To assess the compliance of ICT products, services and processes, as well as managed services in the field of security of cybersecurity management systems and individuals, interested entities will be required to obtain prior PCA accreditation. Further, the PCA will be obliged to provide information on applications for accreditation that are granted and refused.

Handling of complaints

Two independent complaint procedures are envisaged. Under the first one, the deadline by which the authority should respond to a complaint is set. Under the second, a complaint may be lodged about the excessive length of the proceedings, if the interested person has a legal interest[1]. Article 24 of the Act deals with the first procedure, under which any entity may lodge a complaint against the actions of the certification body. The resolution of the complaint should take no longer than 2 months and the complaint itself should be examined by persons other than those who were originally involved in the certification procedure. According to the regulations, the Minister is the authority competent to examine complaints against entities that have issued compliance declarations.

Administrative penalties

The Act also introduces administrative penalties for failure to comply with certain obligations, including for a compliance assessment institution that issues a certificate despite operating without the required accreditation, for a compliance assessment entity which, although obliged to do so, does not provide the data required under the Act, or for ICT product providers that do not perform the obligations related to tests carried out to determine compliance with the requirements of a given European certification programme or in the national cybersecurity certification scheme[2]. Failure by compliance assessment institutions or providers of ICT products and services to perform their obligations, such as the provision of false data or lack of

[1] Article 26 in conjunction with Article 25 of the Act.
[2] Articles 28 and 33 of the Act.

CLIFFORD
CHANCE

required accreditation, may result in a fine of up to 20 times the average salary announced by the President of the Central Statistical Office in the Official Journal of the Republic of Poland 'Monitor Polski' for the year preceding the year of imposing the financial penalty[3].

What next?

The entry into force of the Act – on 28 August 2025 - opens a new chapter for enterprises and the administration. The activities of the Ministry of Digital Affairs, which will prepare the national certification schemes and ensure effective supervision, will be key. However, it is already worth analysing now how certification can translate into a market advantage, as well as how to adapt your products and services to future requirements.

The new Act not only increases the level of cybersecurity in Poland, but also provides a real opportunity to strengthen the position of Polish companies on the demanding, increasingly aware European market – and trust and digital security are already becoming key competitive advantages.

CONTACT

Agnieszka Janicka
Partner

T +48 22 627 11 77
E agnieszka.janicka
@cliffordchance.com

Krzysztof Hajdamowicz
Counsel

T +48 22 627 11 77
E krzysztof.hajdamowicz
@cliffordchance.com

Martyna Sieczka
Associate

T +48 22 627 11 77
E martyna.sieczka
@cliffordchance.com

Agata Wężyk
Legal Intern

T +48 22 627 11 77
E agata.wezyk
@cliffordchance.com

[3] Article 2, item 19 of the Act.

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2025

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest** • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague** • Riyadh* • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

**Clifford Chance has entered into association agreements with Clifford Chance Prague Association SRO in Prague and Clifford Chance Badea SPRL in Bucharest.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.