FUNKCJE PRAWA KARNEGO W EHDS

KONFERENCJA: Europejska przestrzeń danych dotyczących zdrowia. Wtórne przetwarzanie danych osobowych oraz prawa osób fizycznych

25.03.2026 r.

dr Katarzyna Syroka-Marczewska

WPiA
UW

EHDS

(1) Celem niniejszego rozporządzenia jest ustanowienie europejskiej przestrzeni danych dotyczących zdrowia (zwanej dalej „EPDZ”), aby poprawić dostęp osób fizycznych do ich elektronicznych danych osobowych dotyczących zdrowia i kontrolę nad nimi w kontekście opieki zdrowotnej), jak również dla lepszego osiągnięcia innych celów przy wykorzystaniu elektronicznych danych dotyczących zdrowia w sektorach opieki zdrowotnej i opieki, które przyniosłyby korzyści społeczeństwu, takich jak badania naukowe, innowacje, kształtowanie polityki, gotowość na zagrożenia dla zdrowia i reagowanie na nie, w tym w celu zapobiegania przyszłym pandemiom i radzenia sobie z nimi, bezpieczeństwo pacjentów, medycyna personalizowana, statystyka publiczna lub działania regulacyjne. Ponadto celem niniejszego rozporządzenia jest poprawa funkcjonowania rynku wewnętrznego poprzez ustanowienie jednolitych ram prawnych i technicznych, w szczególności w zakresie rozwoju, wprowadzania do obrotu i wykorzystywania systemów elektronicznej dokumentacji medycznej (system EDM) zgodnie z wartościami Unii. EPDZ będzie kluczowym elementem tworzenia silnej i odpornej Europejskiej Unii Zdrowotnej.

(4) Biorąc pod uwagę wrażliwość elektronicznych danych osobowych dotyczących zdrowia, niniejsze rozporządzenie ma na celu zapewnienie wystarczających zabezpieczeń zarówno na poziomie unijnym, jak i krajowym, aby zapewnić wysoki poziom ochrony, bezpieczeństwa, poufności i etycznego wykorzystywania danych. Takie zabezpieczenia są niezbędne, aby wspierać zaufanie do bezpiecznego przetwarzania elektronicznych danych dotyczących zdrowia osób fizycznych do pierwotnego wykorzystywania i wtórnego wykorzystywania w rozumieniu niniejszego rozporządzenia.

EHDS

(11) Niniejsze rozporządzenie nie ma wpływu na kompetencje państw członkowskich w zakresie wstępnej rejestracji elektronicznych danych osobowych dotyczących zdrowia, takie jak uzależnianie rejestracji danych genetycznych od zgody osoby fizycznej lub innych zabezpieczeń. Państwa członkowskie mogą wymagać, aby dane były udostępniane w formacie elektronicznym przed rozpoczęciem stosowania niniejszego rozporządzenia. Nie narusza to obowiązku udostępniania w formacie elektronicznym danych osobowych dotyczących zdrowia zarejestrowanych po dniu rozpoczęcia stosowania niniejszego rozporządzenia.

(45) Należy jasno i proporcjonalnie rozdzielić obowiązki odpowiadające roli poszczególnych podmiotów gospodarczych w procesie dostawy i dystrybucji systemów EDM. Podmioty gospodarcze powinny odpowiadać za wywiązywanie się z obowiązków przypisanych do ról, które pełnią w takim procesie, oraz powinny zapewnić, aby udostępniały na rynku wyłącznie systemy EDM spełniające odpowiednie wymogi.

(52) Niniejsze rozporządzenie nie utrudnia stosowania ani nie zastępuje istniejących uzgodnień umownych lub innych mechanizmów, lecz ma na celu ustanowienie wspólnego mechanizmu dostępu do elektronicznych danych dotyczących zdrowia do wtórnego wykorzystywania w całej Unii.

FUNKCJE PRAWA KARNEGO

- FUNKCJA SPRAWIEDLIWOŚCIOWA
- FUNKCJA OCHRONNA
- FUNKCJA GWARANCYJNA

KODEKS KARNY

Art. 268. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego.

Art. 268a. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

KODEKS KARNY

Art. 269. § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269a. Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

KODEKS KARNY

Art. 269b. § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2, art. 269a, art. 270 § 1 albo art. 270a § 1, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 1a. Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

Art. 269c. Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

USTAWA O OCHRONIE DANYCH OSOBOWYCH

Art. 107. 1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

PRZYSZŁOŚĆ

?

DZIĘKUJĘ

k.syroka-marczewska@wpia.uw.edu.pl