



**Zadania administratorów i IOD  
w kontekście bezpiecznego  
przetwarzania danych osobowych**

**20 września 2022 r.**



### O badaniu:

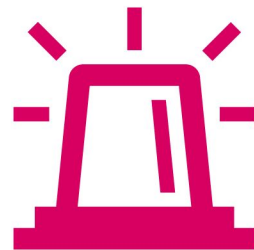


Przeprowadzone w I połowie 2022 roku na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu Ochrony Danych Osobowych, metodą CAWI na reprezentatywnej grupie 1010 respondentów przez IMAS International.



Efektem badania są trzy raporty „Wiedza na temat bezpieczeństwa danych osobowych w Polsce” (maj 2022 r.), „Cyberzagrożenia – czego boją się Polacy?” (czerwiec 2022 r.) oraz „Zadania administratorów i inspektorów ochrony danych osobowych” (wrzesień 2022 r.).

# Jak poradzić sobie z konsekwencjami wycieków?



Tylko niewiele ponad **30% ankietowanych** wie, kto powinien się zająć przeciwdziałaniem negatywnych skutków wycieków.

# Kto się powinien zająć neutralizacją skutków wycieku?

Firma lub instytucja, która jest administratorem danych, które wyciekły.

Inspektorzy ochrony danych osobowych z instytucji lub firmy, z której dane wyciekły.

70%

Policja i inne służby ścigania, np. prokuratura.

60%

56%

Urząd Ochrony Danych Osobowych.

44%

# Kto się powinien zająć neutralizacją skutków wycieku?



**35% badanych**, którzy twierdzą, że wiedzą, kto powinien się tym zająć uważa, że to zadanie poszkodowanych.

# Co w przypadku wycieku powinien zrobić administrator bazy danych?

63%

Poinformować o wycieku.

53%

Poinformować do kogo trafiły dane.

60%

Poinformować jakie dane wyciekły.

48%

Poinformować o możliwych skutkach.

57%

Wdrożyć działania, które zmniejszą ryzyko ponownego wycieku.

44%

Zarekomendować działania, które pomogą zminimalizować skutki wycieku.

# Wyciek danych – skutki i konsekwencje

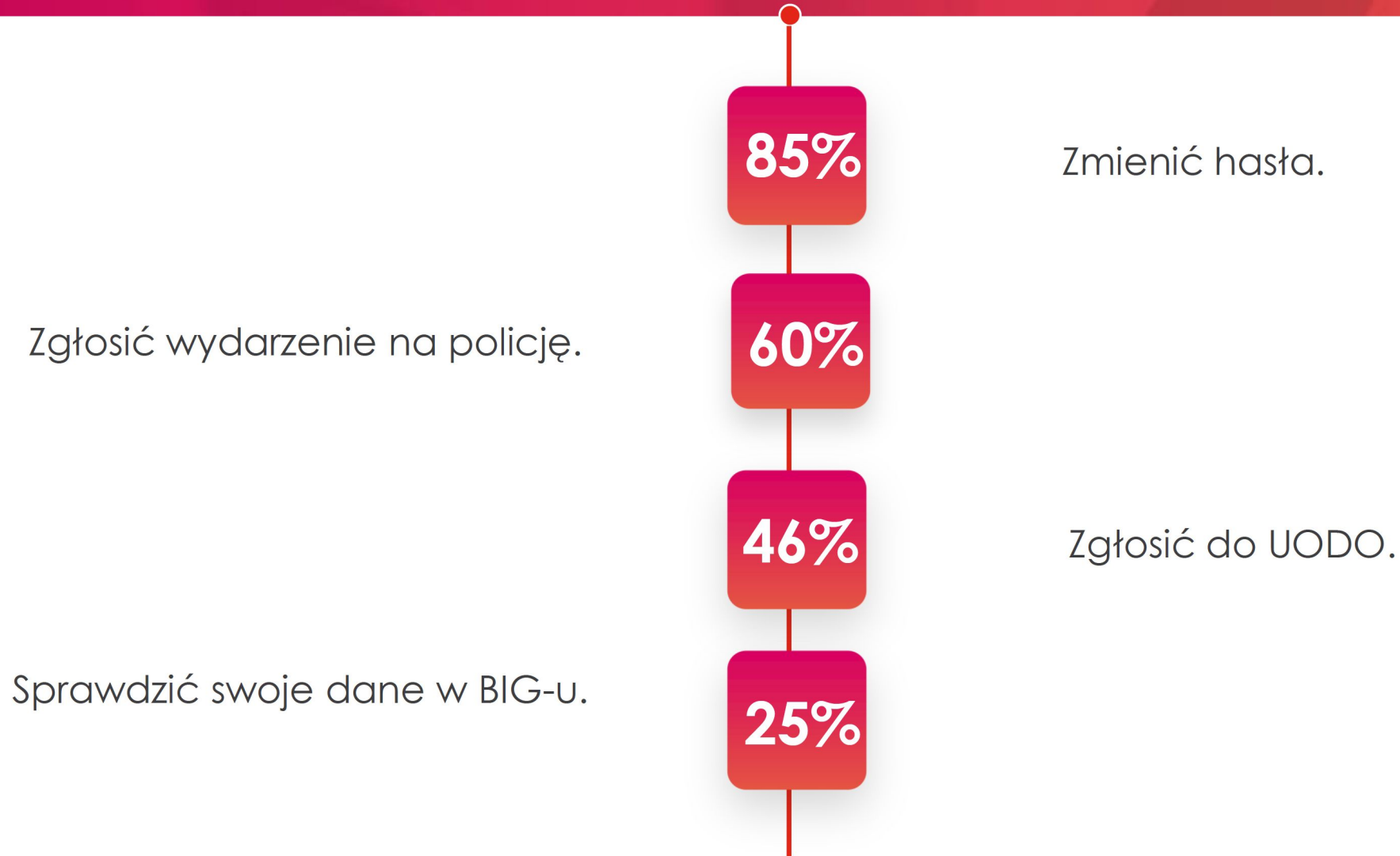


**46% ankietowanych** wie, jakie działania należy podjąć w przypadku wycieku danych.



**2/3 ankietowanych** deklaruje, że wie, jakie mogą być konsekwencje wycieku danych osobowych.

# Jak konkretnie reagować?





# Jak przestępcy mogą wykorzystać dane osobowe

Mogą podszywać się pod nas, próbować oszukać naszych przyjaciół lub rodzinę.

Mogą założyć firmę na nasze dane, na którą zaciągną kolejne zobowiązania finansowe.

86%

Mogą zaciągnąć zobowiązanie finansowe na wyłudzone dane.

75%

68%

Mogą sprzedać wyłudzone dane.

64%

51%

Mogą nas szantażować w celu uzyskania korzyści finansowych.

# Czego od administratora bazy danych oczekują osoby, których dane wyciekły?



**53% ankietowanych** oczekiwałoby wsparcia prawnego.

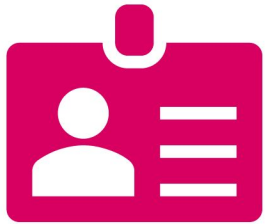


**52% badanych** oczekiwałoby pokrycia kosztów wsparcia prawnego oraz ewentualnych konsekwencji wycieku.

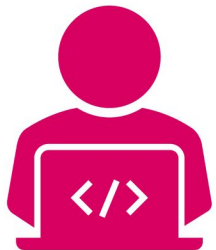


**39% ankietowanych** chciałoby otrzymać rekompensatę finansową lub rabat na usługi firmy, z której dane wyciekły.

# Ochrona danych osobowych w miejscu pracy



Prawie **70% ankietowanych** deklaruje, że zna zasady ochrony danych osobowych w swoim miejscu pracy.



Ponad **60% badanych** wie, do kogo w firmie powinna zgłosić przypadki wycieków lub incydentów bezpieczeństwa.

# Ochrona danych osobowych w miejscu pracy



**51% respondentów** deklaruje, że nie wie, w jaki sposób pracodawca zabezpiecza ich dane osobowe.



Tylko **39% badanych** potwierdza, że pracodawca zapewnia im regularne szkolenia na temat bezpieczeństwa danych.

# DZIĘKUJĘ ZA UWAGĘ!

**Andrzej Kulik**

Dyrektor Departamentu

Analiz Rynkowych i Komunikacji

e-mail: [a.kulik@krd.pl](mailto:a.kulik@krd.pl)

kom. 661 948 058



CHRONPESEL.PL

