FUNDACJA
bezpieczna
cyberprzestrzeń

Przetwarzanie danych w chmurze a bezpieczeństwo informacji

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Różny stopień wrażliwości danych

Maskowanie lub deidentyfikacja

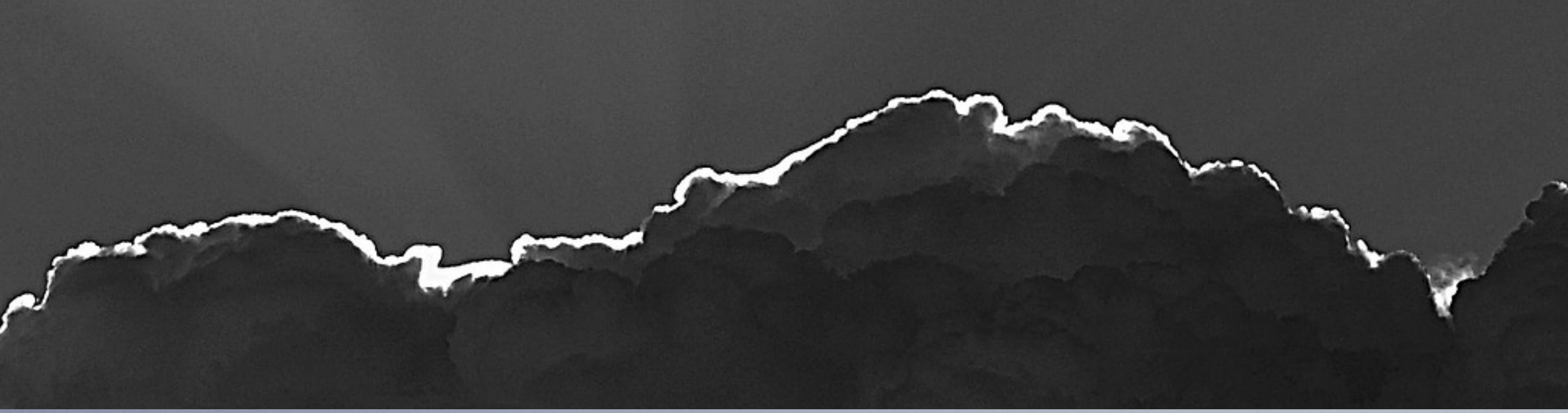
Transport (wprowadzanie, sięganie)

Dane w spoczynku (retencja, usuwanie)

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

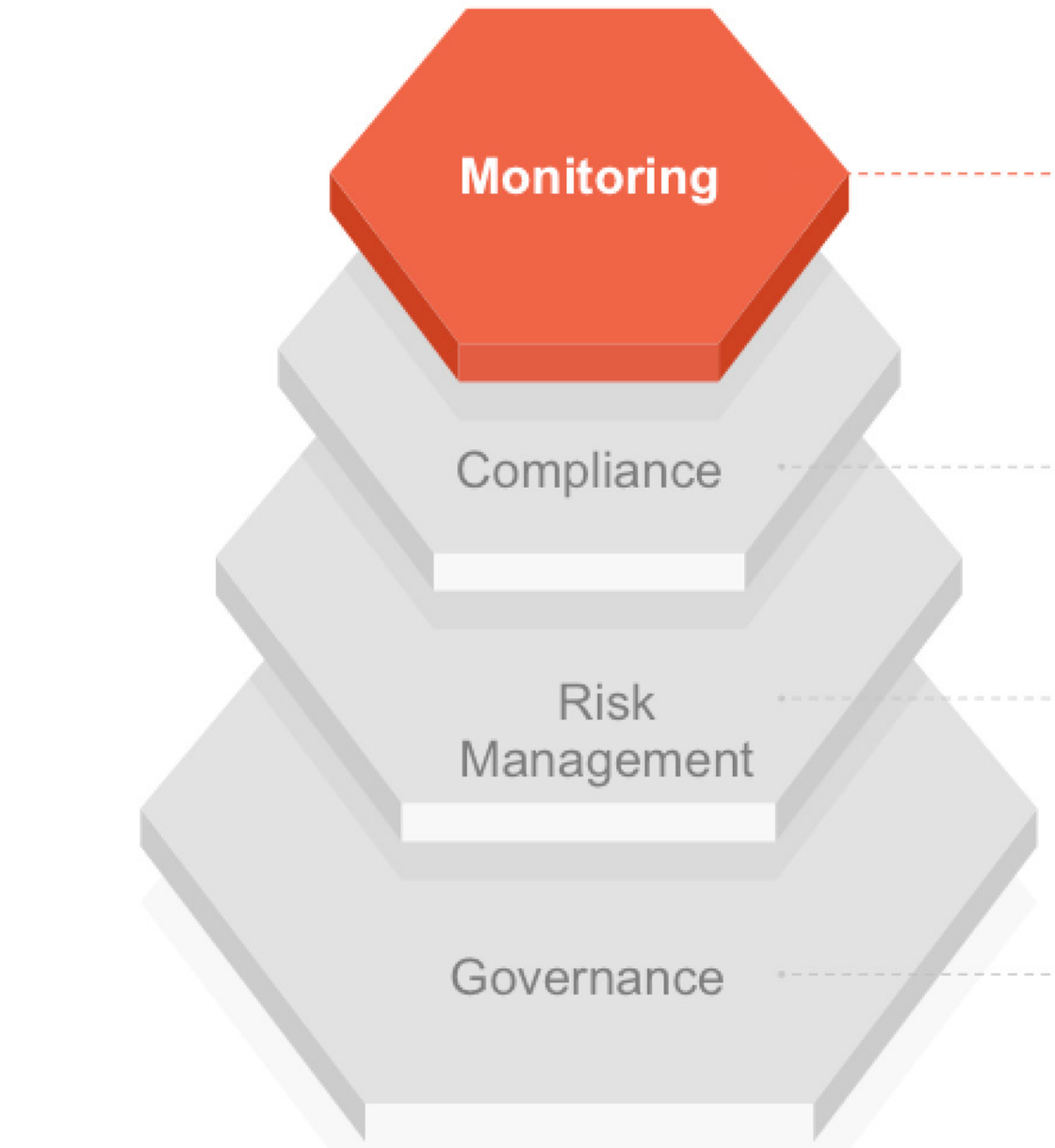
Jachranka, 27 listopada 2015r.

Analiza GRC



T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.



Analiza ciągłości działania

Zaangażowanie, dyspozycyjność
Obsrwacja rynku, uzależnienie od dostawcy
Metodyka pracy, kontrola

Zgodność

Legislacja, wew. Wymagania prawne
Zalecenia, dobre praktyki
Wydatki w przypadku naruszenia

Zarządzanie ryzykiem

Identyfikacja, analizy
Szacowanie ryzyka
Certyfikacja, standardy, kontrola

Ład korporacyjny

Procedury, polityki
Decyzje, instrukcje
Strategia

Źródło: Beata Marek, cyberlaw.pl

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Umowa wynegocjowana

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Opinia Grupy Roboczej art. 29 w sprawie przetwarzania danych w chmurze obliczeniowej 5/2012

Umowa powierzenia powinna zawierać:

1. Szczegółowe informacje na temat (zakresu i rodzajów) **instrukcji klienta** dla dostawcy w ramach świadczenia usługi
2. infromacje na temat gwarantowanego poziomu usług (**SLA**)
3. **sankcje** finansowe lub inne w przypadku braku zapewnienia zgodności przez przetwarzającego
4. określenie **środków bezpieczeństwa** wdrożonych przez przetwarzającego (co najmniej takich jak ma wdrożone ADO)
5. **ramy czasowe** umowy o świadczenie usługi
6. **rodzaje** przetwarzanych danych, **zakres, cel i sposób przetwarzania**

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Opinia Grupy Roboczej art. 29 w sprawie przetwarzania danych w chmurze obliczeniowej 5/2012

7. określenie warunków **wyjścia/migracji/usunięcia** danych (na wniosek)
8. określenie **klauzuli poufności** (osoby upoważnione mogą mieć dostęp)
9. obowiązek **współpracy** przetwarzającego w zakresie zapewnienia realizacji praw osób, których dane dotyczą (np. prawo dostępu do treści swoich danych)
10. brak możliwości **przekazywania danych osobom trzecim**, nawet w celach zatrzymania.
11. **zgodę /sprzeciw** dla podpowierzenia
12. **wykaz podmiotów**, którym przetwarzający zamierza podpowierzać przetwarzanie danych osobowych + zobowiązanie do takich samych zapisów
13. obowiązek **informowania** ADO o każdym naruszeniu przetwarzania danych (w tym kontroli przetwarzania przez organ typu GIODO)

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Opinia Grupy Roboczej art. 29 w sprawie przetwarzania danych w chmurze obliczeniowej 5/2012

14. wskazanie **listy lokalizacji**, w których dane mogą być przetwarzane
15. prawo do **monitorowania/kontrolowania** przetwarzającego przez ADO
16. zobowiązanie przetwarzajacego, że w przypadku wdrożenia dodatkowych funkcji czy innych **istotnych zmian w umowie** musi poinformować on o tym ADO przed ich wdrożeniem (a ADO może od umowy odstąpić)
17. prawo do **rejestru i kontroli istotnych operacji** przetwarzania danych
18. zobowiązanie przetwarzającego do **informowania o każdym wniosku udostępniania danych** o ile nie jest to prawnie zabronione (prawo właściwe!)
19. oświadczenie, że **wewnętrzne procedury i organizacja pracy** przetwarzającego jest zgodna z prawem właściwym dla ADO (+wyniki audytów)
20. zobowiązanie do zachowania **integralności, poufności, rozliczalności, przejrzystości** przetwarzania danych

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

21. zobowiązanie, że dane zostaną **odizolowane** (chmura prywatna, różne poziomy dostępów do danych, odpowiednie zarządzanie współdzielonymi zasobami)
22. szczegółowe adnotacje na temat **transferu poza EOG**, a w przypadku informacji o certyfikacji ADO powinien **załączyć dowód** + określić szczegółowe postanowienia związane z bezpieczeństwem
23. zobowiązanie, że dane nie będą przekazywane do **państw trzecich** bez zapewniania dodatkowych **gwarancji** (jak wyżej)
24. w przypadku transgranicznego przekazywania danych wyjściowe są **SCC**
25. zobowiązanie do ponoszenia **odpowiedzialności/współodpowiedizalności** przetwarzającego
26. w przypadku braku oparcia się na SCC wdrożenie na **BCR**

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Memorandum Sopockie

Przed podpisaniem umowy należy sprawdzić:

1. Czy powierzenie przetwarzania może prowadzić do obniżenia **standardów**?
2. Czy została przeprowadzana **analiza ryzyka** (w tym PIA)?
3. Czy **klauzule umowne** są negocjowalne? Czy odpowiadają naszej zgodności?
4. Jakie **procedury** w celu ochrony danych wdrożył przetwarzający?
5. Czy jest **certyfikowany**?
6. Czy są prowadzone i udostępniane **dzienniki lokalizacji danych**?
7. Czy jest prowadzony i udostępniany automatycznie **rejestrowany dziennik kontroli kopiowania i usuwania**?
8. Czy są sporządzane **kopie zapasowe** powyższych dokumentów?
9. Jakiego rodzaju **środki techniczne** są wdrożone w celu zabezpieczenia danych i nie przekazywania ich do jurysdykcji państw trzecich?

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Memorandum Sopockie

Przed podpisaniem umowy należy sprawdzić:

10. Czy dane są **usuwane** w skuteczny sposób, np. poprzez natychmiastowe nadpisanie losowych danych?
11. Czy dane w spoczynku i transporcie są **szyfrowane**?
12. Czy jest prowadzona i udostępniana automatyczna **rejestracja danych każdego przetworzenia danych**?

Umowa powierzenia powinna zawierać:

1. informacje na temat wszystkich **fizycznych lokalizacji** przetwarzania danych
2. zobowiązanie do **nieprzekazywania danych** poza tę lokalizację (np. EOG)

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Memorandum Sopockie

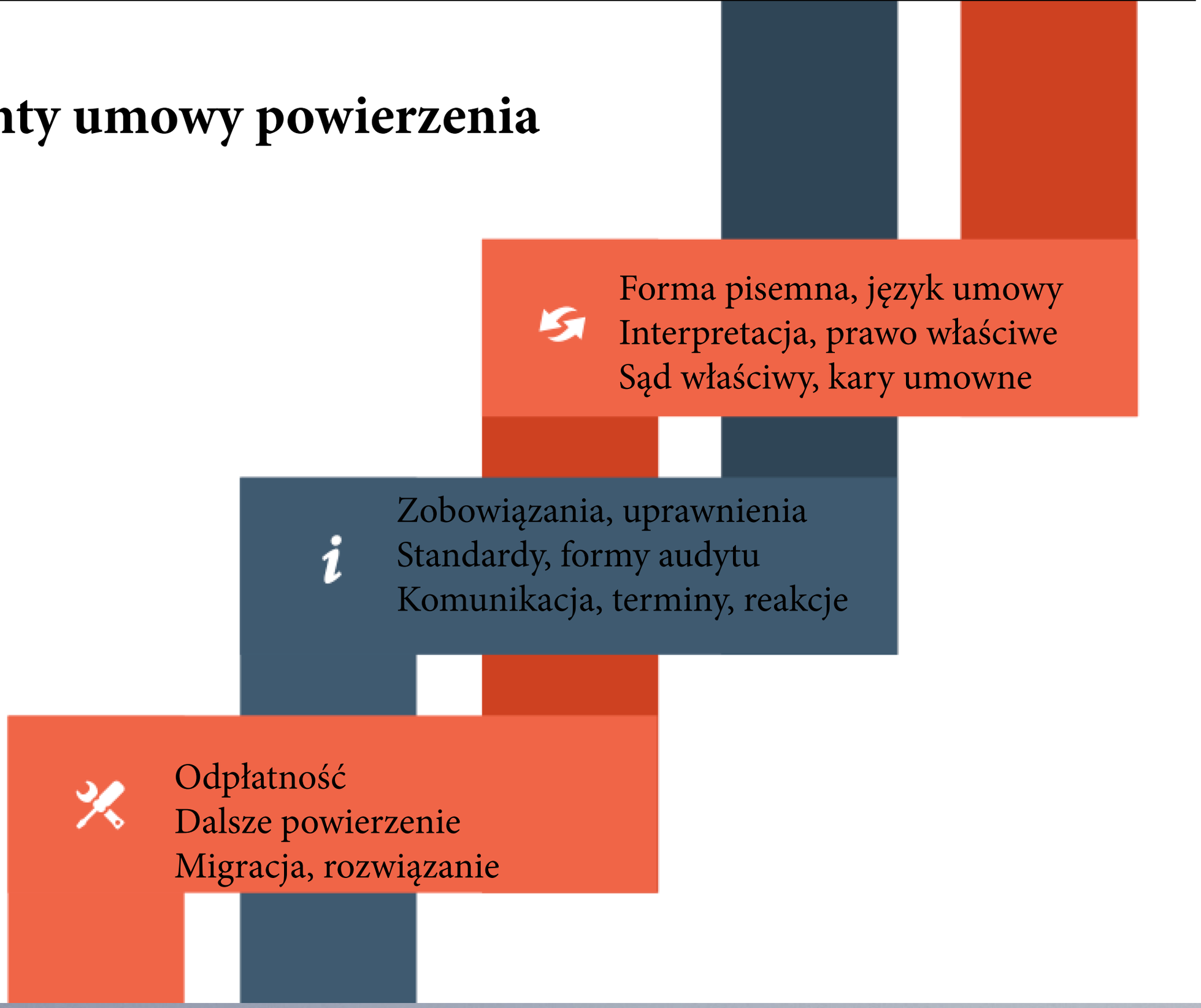
Umowa powierzenia powinna zawierać:

3. zobowiązanie do przetwarzania danych zgodnie z **instrukcjami ADO**
4. uprawnienie do **rozwiązania umowy, migracji** danych w przypadku jednostronnej zmiany umowy przez przetwarzającego
5. zobowiązanie do przetwarzania zgodnie z **celami** wskazanymi przez ADO
6. uprawnienie prawa **wglądu/sprawdzenia lokalizacji** przetwarzania (!)
7. uprawnienie do przeprowadzania **audytów** przez zaufane podmioty
8. zapisy aby uniknąć uzależnienia od dostawcy usług w chmurze (**lock-in**)
9. zapisy dotyczące **współdziałania/procedur działania pomiędzy stronami** (ADO musi mieć możliwość prawidłowo realizować swoje obowiązki prawne)

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Elementy umowy powierzenia



T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Risk Based Approach w inteligentnych sieciach

* charakter
* zakres
* kontekst
* cele

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

Case study: problem wyjścia

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.

FUNDACJA
bezpieczna
cyberprzestrzeń

Dziękuję za uwagę

T: (+48) 500-435-372
E: beata.marek@cyberlaw.pl

Jachranka, 27 listopada 2015r.