

Przykłady naruszenia ochrony danych osobowych	
1	stwierdzono naruszenie zabezpieczenia systemu informatycznego lub urządzeń, nośników przetwarzających dane (laptop, telefon, pendrive, dysk zewnętrzny itp.)
2	sposób działania programu lub jakość komunikacji w sieć telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych,
3	nieuprawnione ujawnienia danych osobowych,
4	udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym,
5	zabrania danych przez osobę nieupoważnioną,
6	niewłaściwe zabezpieczenie fizyczne pomieszczeń lub dokumentacji,
7	nieodpowiednie zabezpieczenie sprzętu IT czy oprogramowania,
8	nieprawidłowe zaadresowanie korespondencji elektronicznej,
9	nieautoryzowany dostęp do systemów informatycznych i urządzeń przetwarzających dane
10	nieautoryzowane modyfikacje lub zniszczenie,
11	pozyskiwanie informacji z nielegalnych źródeł
12	nieupoważniony dostęp, modyfikację, kopiowanie lub zniszczenie/usunięcie danych osobowych
13	niekopertowanie danych wrażliwych w trakcie przenoszenia,
14	pozostawiania danych w miejscu ogólnie dostępnym (np. na drukarkach,kopiarkach)
15	zgubienie pendriva, laptopa lub innego nośnika,
16	nieautoryzowany dostęp do danych przez połączenie sieciowe,

17	dostęp do pomieszczeń, w których przetwarza się dane osobowe dla osób nieuprawnionych,
18	niezablokowanie dostępu do systemu,
19	brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach gdzie przetwarza się dane osobowe,
20	wykrycie niezabezpieczonego kanału dystrybucji danych osobowych,
21	nielegalne bądź nieświadome ujawnienie danych osobowych,
22	pozyskiwanie danych osobowych z nielegalnych źródeł,
23	przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem,
24	stwierdzenie obecności wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego,
25	ujawnienie indywidualnych haseł dostępu do systemu,
26	przesyłanie danych osobowych przez Internet bez zabezpieczenia,
27	niestosowanie zasady czystego biurka i czystego ekranu,
28	przesyłanie dokumentów papierowych i nośników elektronicznych z danymi bez zabezpieczenia,
29	wykonanie nieuprawnionych kopii danych osobowych,
30	naruszenie bezpieczeństwa kopii danych osobowych,
31	kradzież nośników zawierających dane osobowe,
32	kradzież sprzętu służącego do przetwarzania danych osobowych,
33	utratę danych osobowych w systemie informatycznym, na kopiach bezpieczeństwa i na innych nośnikach,
34	brak aktualnych kopii bezpieczeństwa danych osobowych

35	niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt,
36	naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe,
37	dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień,
38	nie zawarcie umowy powierzenia z firmami współpracującymi (serwis, naprawa i inne),
39	przekazanie danych osobowych za pośrednictwem osób nieupoważnionych,