UNIWERSYTET
KARDYNAŁA STEFANA WYSZYŃSKIEGO
W WARSZAWIE

OCHRONA DANYCH OSOBOWYCH

PORADNIK

w.1.1/2020

SIEĆ I CHMURA

- używaj tylko **zaufanego dostępu** do sieci (bezpieczne hasło, aktualne oprogramowanie routera)
- korzystając z ogólnodostępnych sieci koniecznie **używaj VPN**, aby Twój ruch sieciowy był szyfrowany
- zwracaj uwagę na **certyfikaty stron** - “zielone kłódeczki”, szczególnie gdy podajesz na nich swoje dane
- **nie klikaj** w dziwne i podejrzane linki
- **dokładnie analizuj** komunikaty od administratora, zawarte np. w wiadomościach SMS, e-mail, by uniknąć np. ataku phishingowego
- **zadbaj** by przechowywane przez Ciebie dane były w bezpieczny sposób zarchiwizowane

Zgodnie z wytycznymi UODO - „Jak chronić swoje dane osobowe ?” - https://uodo.gov.pl/pl/138/1221

NARZĘDZIA INFORMATYCZNE

- **używaj wskazanych przez Uniwersytet** do przeprowadzenia zajęć, egzaminów i zaliczeń zajęć na ocenę, narzędzi USOSweb Uniwersytetu, tj. MS Office 365, MS Teams, Platforma Moodle
- **archiwizuj dokumentację** z egzaminów i zaliczeń na platformie Moodle lub w innej formie, pozwalającej dokonać weryfikacji (dysk OneDrive, nośniki elektroniczne). Czas archiwizacji na Wydziale to 3 lata.

Decyzja Nr 7/2020 Prorektora ds. Studenckich i Kształcenia Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie z dnia 29 kwietnia 2020 r. w sprawie zaliczania zajęć i przeprowadzania egzaminów z wykorzystaniem technologii informatycznych zapewniających kontrolę ich przebiegu i rejestrację.

URZĄDZENIA

- jeśli pracujesz na prywatnym komputerze **upewnij się**, że masz zainstalowane wszystkie najnowsze aktualizacje do swojego systemu operacyjnego i program antywirusowy
- do pracy zdalnej na domowym komputerze **załóż** sobie **inne konto użytkownika zabezpieczone hasłem**
- gdy masz dostęp do aplikacji UKSW (np. USOS, dyski sieciowe) **nie dawaj dostępu** do komputera innym osobom
- ustaw hasło na swojego użytkownika i odchodząc od komputera **zawsze blokuj** ekran (WinKey + L / Control-Command-Q)

Zarządzenie Nr 40/2018 Rektora Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie z dnia 21 września 2018 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

URZĄDZENIA, cd.

- **zabezpieczaj komputer** poprzez używanie silnych haseł dostępu, aby ograniczyć ryzyko utraty danych w przypadku jego kradzieży lub zgubienia
- jeśli urządzenie na którym pracujesz zostało skradzione, jeśli to możliwe **postaraj się zdalnie wyczyścić jego pamięć**
- podejmij **szczególne środki ostrożności** (szyfruj pliki z danymi) by urządzenia z których korzystasz i te które służą do przenoszenia danych nie zostały zgubione

Zarządzenie Nr 40/2018 Rektora Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie z dnia 21 września 2018 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie

EMAIL

- do kontaktu ze studentami/słuchaczami służy moduł USOSMail. **Nie kopiuj adresów** e-mail z USOS-a do innego programu, w celu wysyłki korespondencji
- **używaj służbowych kont email** w domenie UKSW. Jeśli musisz skorzystać z prywatnego konta e-mail unikaj używania danych osobowych lub wrażliwych w treści lub temacie wiadomości
- w przypadku wysyłania korespondencji do większej liczby osób, **zadbaj o to, aby osoba**, do której skierowana jest tego typu korespondencja, **nie miała możliwości zapoznania się z danymi** pozostałych adresatów — nie tylko ich imionami i nazwiskami, ale również adresami e-mail
- przy wysyłce korespondencji do wielu adresatów **stosuj opcję „kopii ukrytej”** (BBC/UDW)

Par. 25 ust. 3 Załącznika nr 1 do Zarządzenia Nr 40/2018 Rektora UKSW z dnia 21 września 2018 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie; Decyzja Nr 1/2016 Rektora UKSW z dnia 7 stycznia 2016 r. w sprawie zasad ujednolicenia adresów kont poczty elektronicznej oraz prowadzenia elektronicznej korespondencji służbowej w Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie /z pozn zm./

EMAIL, cd.

- **upewnij się**, że wysyłasz wiadomość do właściwego adresata, zwłaszcza jeśli zawarte są w niej dane osobowe lub wymagające szczególnej ochrony
- **dokładnie sprawdź nadawcę** maila. **Nie otwieraj** wiadomości od nieznanych adresatów, a zwłaszcza załączników. **Nie klikaj w link** zawarty w podejrzanej wiadomości. To może być atak phishingowy
- **nie przesyłaj wiadomości zaszyfrowanej razem z hasłem**, nawet w osobnej wiadomości. Ten kto ma dostęp do Twojej poczty bez problemu odszyfruje wiadomość.

Par. 25 ust. 3 Załącznika nr 1 do Zarządzenia Nr 40/2018 Rektora UKSW z dnia 21 września 2018 r. w sprawie wprowadzenia Polityki bezpieczeństwa informacji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie; Decyzja Nr 1/2016 Rektora UKSW z dnia 7 stycznia 2016 r. w sprawie zasad ujednolicenia adresów kont poczty elektronicznej oraz prowadzenia elektronicznej korespondencji służbowej w Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie /z pozn zm./

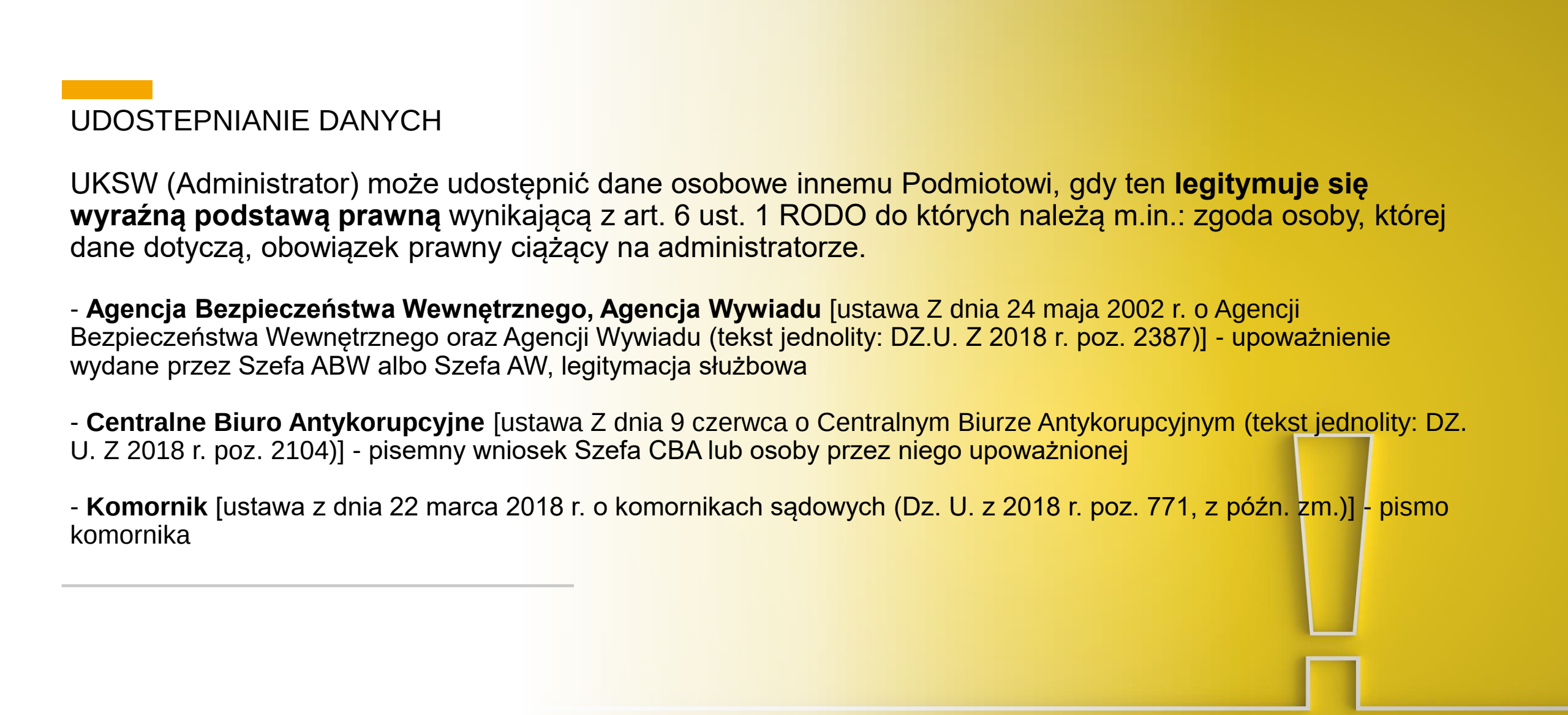
UDOSTEPNIANIE DANYCH

UKSW (Administrator) może udostępnić dane osobowe innemu Podmiotowi, gdy ten **legitymuje się wyraźną podstawą prawną** wynikającą z art. 6 ust. 1 RODO do których należą m.in.: zgoda osoby, której dane dotyczą, obowiązek prawny ciążący na administratorze.

- **Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu** [ustawa Z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jednolity: DZ.U. Z 2018 r. poz. 2387)] - upoważnienie wydane przez Szefa ABW albo Szefa AW, legitymacja służbowa

- **Centralne Biuro Antykorupcyjne** [ustawa Z dnia 9 czerwca o Centralnym Biurze Antykorupcyjnym (tekst jednolity: DZ. U. Z 2018 r. poz. 2104)] - pisemny wniosek Szefa CBA lub osoby przez niego upoważnionej

- **Komornik** [ustawa z dnia 22 marca 2018 r. o komornikach sądowych (Dz. U. z 2018 r. poz. 771, z późn. zm.)] - pismo komornika



UDOSTEPNIANIE DANYCH, cd.

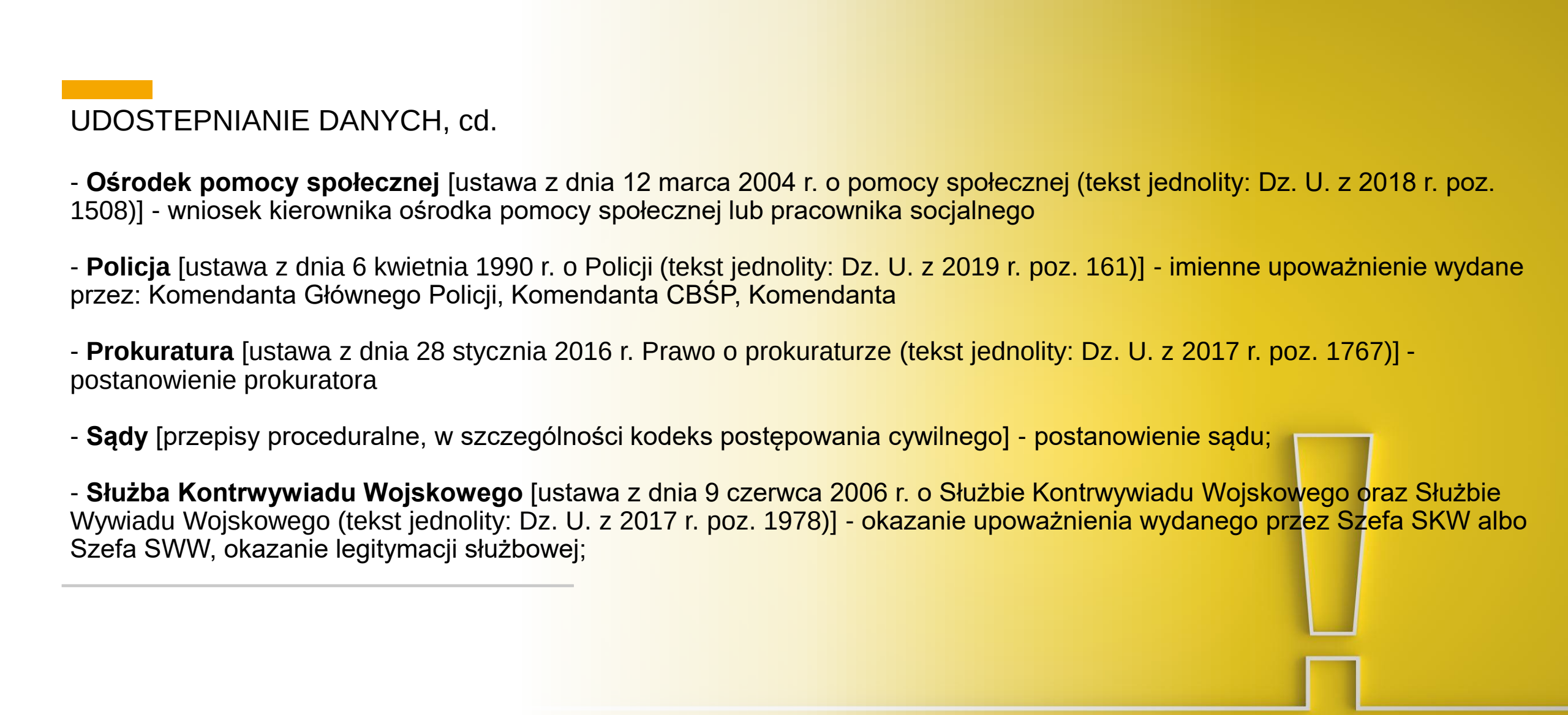
- **Ośrodek pomocy społecznej** [ustawa z dnia 12 marca 2004 r. o pomocy społecznej (tekst jednolity: Dz. U. z 2018 r. poz. 1508)] - wniosek kierownika ośrodka pomocy społecznej lub pracownika socjalnego

- **Policja** [ustawa z dnia 6 kwietnia 1990 r. o Policji (tekst jednolity: Dz. U. z 2019 r. poz. 161)] - imienne upoważnienie wydane przez: Komendanta Głównego Policji, Komendanta CBŚP, Komendanta

- **Prokuratura** [ustawa z dnia 28 stycznia 2016 r. Prawo o prokuraturze (tekst jednolity: Dz. U. z 2017 r. poz. 1767)] - postanowienie prokuratora

- **Sądy** [przepisy proceduralne, w szczególności kodeks postępowania cywilnego] - postanowienie sądu;

- **Służba Kontrwywiadu Wojskowego** [ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (tekst jednolity: Dz. U. z 2017 r. poz. 1978)] - okazanie upoważnienia wydanego przez Szefa SKW albo Szefa SWW, okazanie legitymacji służbowej;

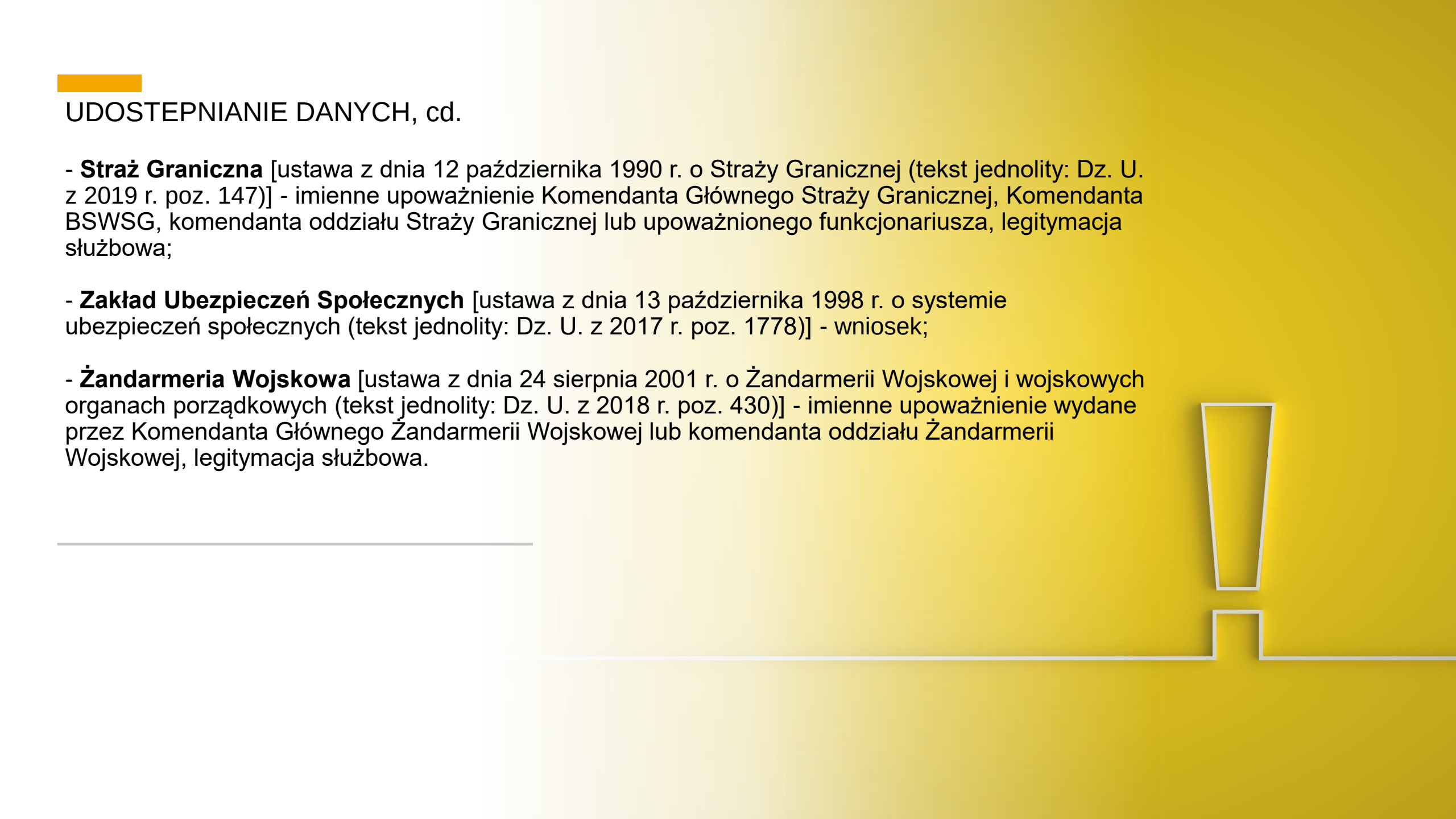


UDOSTEPNIANIE DANYCH, cd.

- **Straż Graniczna** [ustawa z dnia 12 października 1990 r. o Straży Granicznej (tekst jednolity: Dz. U. z 2019 r. poz. 147)] - imienne upoważnienie Komendanta Głównego Straży Granicznej, Komendanta BSWSG, komendanta oddziału Straży Granicznej lub upoważnionego funkcjonariusza, legitymacja służbowa;

- **Zakład Ubezpieczeń Społecznych** [ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (tekst jednolity: Dz. U. z 2017 r. poz. 1778)] - wniosek;

- **Żandarmeria Wojskowa** [ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (tekst jednolity: Dz. U. z 2018 r. poz. 430)] - imienne upoważnienie wydane przez Komendanta Głównego Żandarmerii Wojskowej lub komendanta oddziału Żandarmerii Wojskowej, legitymacja służbowa.

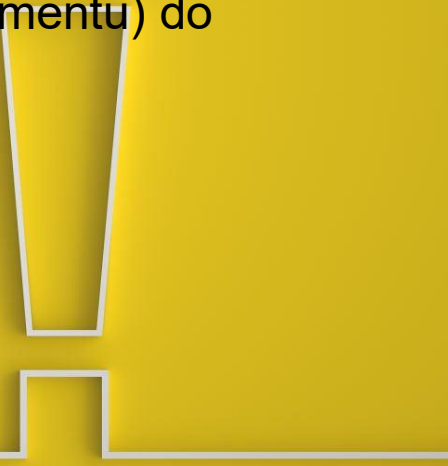


UDOSTEPNIANIE DANYCH, cd.

Udostępnienie danych osobowych, np. o pracowniku, studencie, absolwencie na wniosek strony trzeciej (np. przyszłego pracodawcę, firmę HR lub inne osoby trzecie), **nie posiadającej wyraźnej podstawy prawnej**, może być zrealizowane **na podstawie zgody** na przetwarzanie danych osobowych **wyrażonej UKSW, przez osobę, której dane dotyczą**.

Zgoda osoby, której dane dotyczą może zostać przekazana UKSW, w następujący sposób:

- podpisanie i złożenie zgody osobiście w jednostce organizacyjnej UKSW. Pracownik UKSW ma obowiązek zweryfikować tożsamość osoby składającej zgodę przez wgląd (zabrania się kserowania dokumentu) do dokumentu potwierdzającego tożsamość (dowód osobisty, paszport, legitymacja studencka)



UDOSTEPNIANIE DANYCH, cd.

- przesłanie mailem zgody opatrzonej kwalifikowanym podpisem elektronicznym
- przesłanie zgody przez ePUAP podpisanej profilem zaufanym
- przesłanie mailem skanu zgody Z podpisem (należy zweryfikować czy adres mailowy, z którego otrzymaliśmy zgodę znajduje się w bazie jednostki organizacyjnej lub zażądać przekazania dodatkowych informacji weryfikacyjnych np. data urodzenia, nr PESEL, nr telefonu).

UKSW NIE jest uprawniony do udostępniania danych osobowych osobom trzecim np. na podstawie skanu zgody przesłanej przez osobę trzecią!

UDOSTEPNIANIE DANYCH, cd.

UKSW, jest zobligowany udostępnić dane osobowe na wniosek osoby, której dane dotyczą – zgodnie z art. 15 RODO.

Zgodnie z ww. przepisem osoba, której dane dotyczą jest uprawniona do uzyskania dostępu do swoich danych osobowych, a także ma prawo uzyskać kopię danych osobowych podlegających przetwarzaniu.

W przypadku wątpliwości co do tożsamości osoby fizycznej składającej wniosek o udostępnienie danych osobowych, można zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą (art. 12 ust. 6 RODO).

NARUSZENIE

Przez pojęcie „naruszenia ochrony danych osobowych” należy rozumieć „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych” (art. 4 pkt 12 RODO).

Przykłady:

„naruszenie poufności” – polega na ujawnieniu danych osobowych nieuprawnionej osobie:

- przypadkowe wysłanie danych osobowych pracownika, studenta do niewłaściwego działu firmy lub osoby postronnej
- system informatyczny administratora został zainfekowany złośliwym oprogramowaniem. Po przeprowadzeniu wstępnej analizy administrator stwierdził, że w wyniku działania tego oprogramowania osoba nieupoważniona uzyskała dostęp do danych osobowych.

Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (w skrócie RODO)

NARUSZENIE, cd.

„naruszenie dostępności” – polega na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych:

- zgubienie lub kradzież nośnika zawierającego bazy danych klientów administratora przy braku kopii zapasowej
- pracownik przypadkowo lub osoba nieupoważniona celowo usuwa dane ze zbioru. Administrator próbuje odzyskać dane z kopii zapasowej, jednak jego działania nie przynoszą rezultatu
- wyniku przerwy w dostawie prądu lub ataku typu „odmowa usługi” (tzw. DDoS), administrator tymczasowo lub trwale traci dostęp do danych osobowych

Brak dostępu do danych może mieć znaczący wpływ na prawa lub wolności osób fizycznych.

Jednak nie każda czasowa niedostępność danych jest naruszeniem.

Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (w skrócie RODO)

NARUSZENIE, cd.

Naruszeniem jest tylko taka niedostępność danych, która może stanowić ryzyko dla praw lub wolności osób fizycznych, np. w przypadku szpitala brak dostępu danych pacjentów może prowadzić do uniemożliwienia przeprowadzenia operacji medycznej, a zatem narażenia życia, co należy zaklasyfikować jako wysokie ryzyko dla praw lub wolności osób fizycznych.

Podobnie w przypadku planowanej konserwacji systemu, dane osobowe mogą być niedostępne przez pewien czas i nie należy traktować tego jako naruszenia bezpieczeństwa.

„naruszenie integralności” – polega na zmianie treści danych osobowych w sposób nieautoryzowany:

- pracownik dla żartu zmienia nazwiska klientów poprzez dopisanie litery „s” na końcu każdego z nich.”

Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (w skrócie RODO)

PODSUMOWANIE

Jeśli masz pytania lub wątpliwości związane z ochroną danych osobowych w UKSW to możesz skontaktować się z Inspektorem Ochrony Danych pod adresem iod@uksw.edu.pl lub telefonicznie 22/5619034

Jeśli spotkałeś się z sytuacją naruszenia bezpieczeństwa ochrony danych lub widzisz działania niepożądane to postępuj zgodnie z przyjętą na UKSW procedurą i zgłoś incydent do IOD, za pomocą formularza dostępnego na stronie głównej Uczelni: menu – Uniwersytet – Ochrona Danych Osobowych https://uksw.edu.pl/pl/odo-naruszenia?ticket=ST-123723-KQiFCc5mdWjJ7ZH3eawL-login.uksw.edu.pl

Jeżeli masz pytania lub wątpliwości

- kontakt do Centrum Systemów Informatycznych : csi@uksw.edu.pl tel.: 22/5618921

Decyzja Nr 8/2019 Prorektora ds. Ogólnych i Rozwoju UKSW z dnia 20 listopada 2019 r. w sprawie wprowadzenia Procedury postępowania z naruszeniami w Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie

Opracowanie:

Monika Masiukiewicz, Inspektor Ochrony Danych Osobowych UKSW