Zalecenia dotyczące prowadzenia zajęć w formie zdalnej – niniejsze opracowanie dotyczy jedynie zagadnień związanych z przetwarzaniem danych osobowych w kontekście obowiązującego w tym zakresie prawa i nie uwzględnia ono innych unormowań czy regulacji.

1. Z jakiej platformy korzystać przy prowadzeniu zajęć w formie zdalnej?
    a. Moodle,
    b. Big Blue Button,
    c. MS Teams.

W przypadku Wydziału Sztuk Pięknych dopuszczalne jest również wykorzystanie usług G-Suite w ramach umowy licencyjnej.
W przypadku Centrum Kształcenia w Języku Angielskim Collegium Medicum UMK dopuszczalne jest również wykorzystanie usługi ZOOM w ramach pakietu Lecturio.

W przypadku Wydziału Fizyki, Astronomii i Informatyki Stosowanej dopuszczalne jest również wykorzystanie usługi Webex.

2. Czy można wymagać od studentów ujawnienia imion i nazwisk?
    Nie należy wymagać od studentów podawania imion i nazwisk. Nie jest to wskazane, ponieważ dla celów identyfikacji wystarczającą daną jest numer albumu studenta. Studenci biorący udział w zajęciach on-line powinni na stosowne platformy logować się z wykorzystaniem indywidualnego konta przydzielonego do tego celu przez Uczelnię (np.: USOS mail, konto Office365).

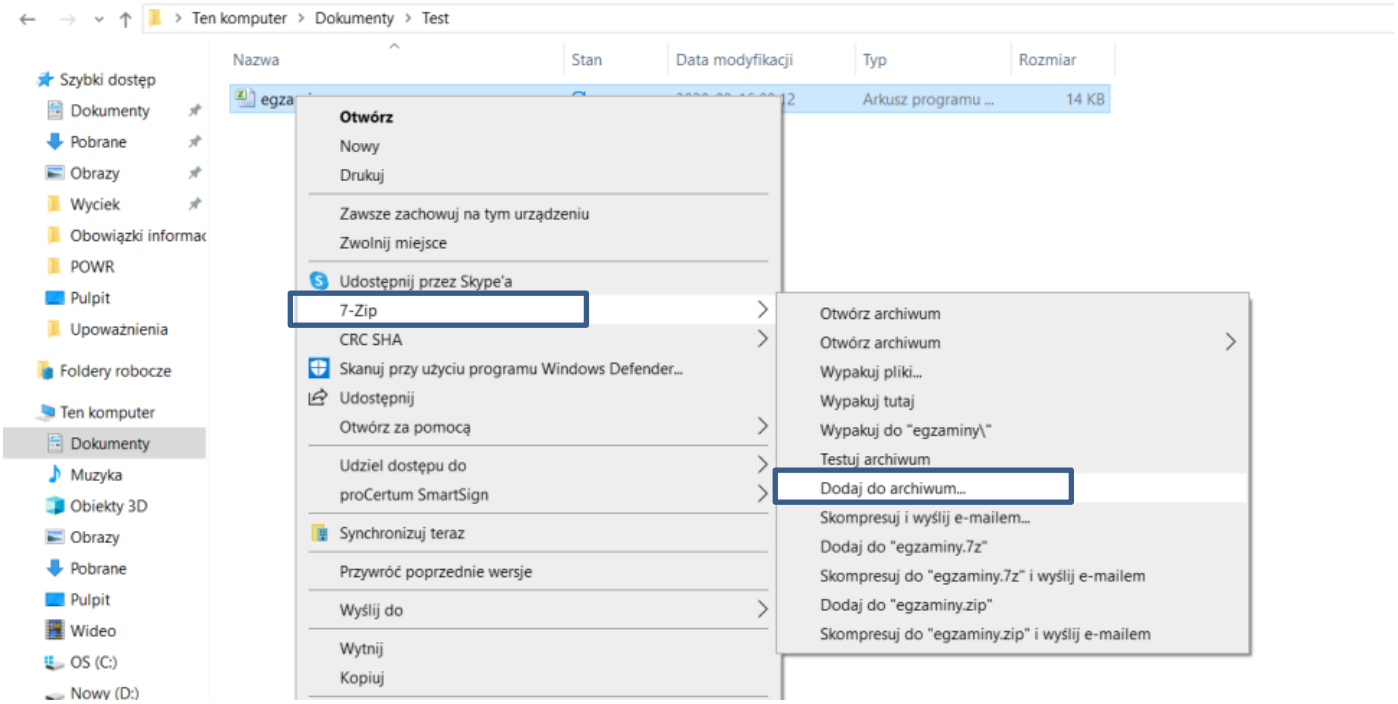
3. Czy można wymagać od studentów ujawniania wizerunku (tj. włączania kamer podczas zajęć prowadzonych w formie zdalnej)?
    Tak. Można wymagać od studentów stosowania kamer i nie narusza to RODO, ani prawa do prywatności. Jest to uzasadnione szczególnie w przypadku gdy obecność na zajęciach jest formą ich zaliczenia, lub oceny cząstkowej.
    Zajęcia może nagrywać jedynie ich organizator i jedynie w celach ściśle związanych z dydaktyką. Nie wolno takich nagrań publikować. Studentów należy poinformować przed uruchomieniem nagrywania o tym fakcie.
    Na początku zajęć należy poinformować studentów, że nagrywanie sesji zajęciowej jest zabronione.

4. W jaki sposób przekazywać dokumenty zawierające dane osobowe za pomocą poczty elektronicznej?

W celu przekazania dokumentów zawierających dane osobowe należy korzystać jedynie z służbowej poczty elektronicznej (w domenie @umk.pl lub @cm.umk.pl). Dokumenty zawierające dane osobowe powinny być zaszyfrowane.

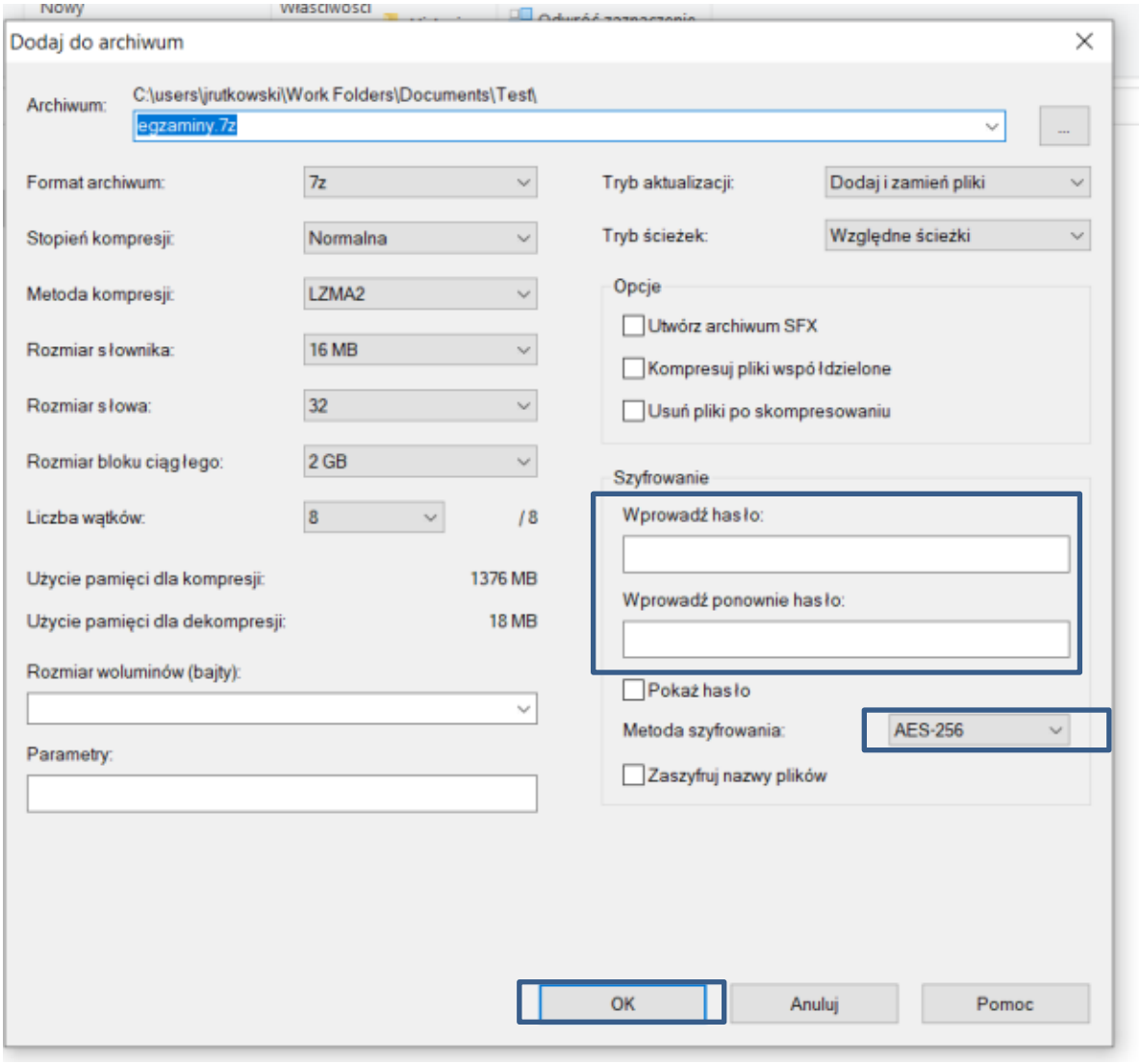
Instrukcja poniżej.

Sposób szyfrowania dokumentów:

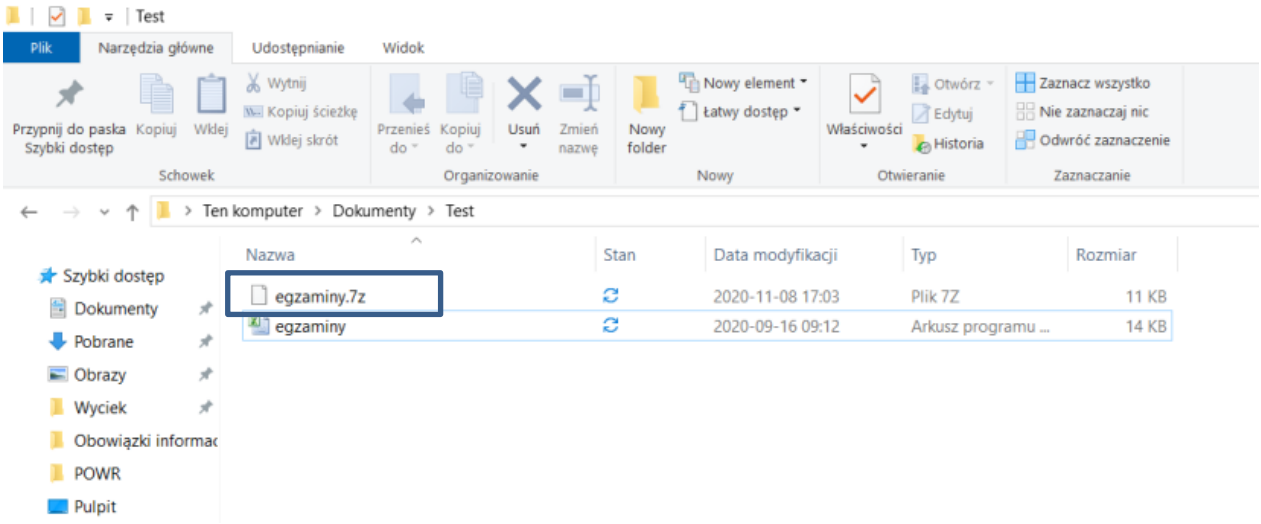


1. Kursorem myszki najeżdżamy na plik zawierający dane osobowe → klikamy prawym przyciskiem myszki → z menu rozwijanego wybieramy 7-zip (RAR, UnRAR, WinZIP, UnZIP) → klikamy lewym przyciskiem myszki na [Dodaj do rachiwum].

2. Po uruchomieniu się okna dialogowego w polu [Wprowadź hasło] wpisujemy hasło. Wprowadzone hasło powtarzamy w polu [Wprowadź ponownie hasło] i klikamy [OK] Należy zwrócić uwagę, żeby [Metoda szyfrowania] pokazywała wartość AES-256, w innym wypadku trzeba wybrać odpowiednią wartość z menu rozwijanego.



3. Tak przygotowany plik (*.7z) dodajemy jako załącznik do wiadomości e-mail.



4. Hasło do odbiorcy dostarczamy innym niż e-mail kanałem. Można na przykład stosować wcześniej umówione hasło. Hasło powinno być skomplikowane (składać się z co najmniej 8 znaków, zawierać przynajmniej: jeden znak specjalny, jedną cyfrę, duże i małe litery).