



Materiały dla studentów

Przewodnik dla studentów PWSZ w Elblągu RODO

Szanowni Studenci w związku z wdrożeniem RODO, przygotowany został przewodnik dla ułatwienia poruszania się studentom po prawach i obowiązkach związanych z RODO. Na stronie internetowej uczelni pojawiła się ikona RODO:

Link + grafika do ikonki

zachęcamy do zapoznania się z zamieszczonymi tam informacjami. W ciągu najbliższych kilku dni pojawią się tam również polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym oraz procedury niezbędne dla funkcjonowania uczelni zgodnie z RODO. Będą to dokumenty jawne, dostępne dla wszystkich.

Rekrutacja studentów:

Studenci biorący udział w rekrutacji powinni podpisać zgodę na przetwarzania danych w celu rekrutacji na studia wraz z informacją, iż jeśli nie zostaną przyjęci na studia ich dane zostaną usunięte najpóźniej rok po rekrutacji. Osoby, które rekrutację przeszły pozytywnie stają się studentami, w ich teczках osobowych powinny się znaleźć wydane przez dziekanat zgody na przetwarzanie danych oraz wykorzystanie wizerunku dla działań marketingowych lub w mediach społecznościowych uczelni podczas studiów.

Koła Naukowe

Studenci zapisujący się do koła naukowego powinni podpisać osobną zgodę na przetwarzanie ich danych przez koło naukowe. Zgoda ta będzie zawierała informacje dotyczące wykorzystania wizerunku dla celów marketingowych koła naukowego (np. zdjęcia z konferencji, wyjazdów, badań et cetera).

Wyjątki od zbierania zgody na wizerunek to: bycie osobą publiczną (np. Rektor uczelni), otrzymanie zapłaty za wystąpienie, bycie tłem jakiejś wypowiedzi (np. wypowiada się Rektor a w tle widać przechodzących korytarzem studentów). Jeśli natomiast to student udziela wypowiedzi np. podczas targów pracy czy konferencji studenckiej niezbędna jest jego pisemna zgoda. Każda zgoda ma swój „termin ważności”:

- skończone studia -> usunięcie zdjęć rok po zakończeniu studiów,
- koło naukowe -> odejście z koła -> usunięcie rok po zakończeniu współpracy.

Wyjeżdżając na wycieczki w ramach studiów, konferencje studenckie możliwe jest robienie zdjęć przez organizatora, to także wykorzystywanie danych studenta przez inne instytucje (np. uczelnie na której odbywa się konferencja, firma do której jest wyjazd, Erasmus) oni także mogą chcieć umieścić



zdjęcia z twoim wizerunkiem, ale powinni wówczas uzyskać zgodę na przetwarzania danych, jednorazową zgodę.

Listy z ocenami

Pracownicy nie będą mogli umieścić w miejscu publicznym listy z ocenami (np. drzwi), każdy student musi się zgłosić do prowadzącego, aby dowiedzieć się o swojej ocenie. Lista ocen w formie mailowej jest dozwolona w przypadku że prowadzący każdemu z osobna udzieli informacji na indywidualnego maila, tylko z jego oceną.

Priorytety dot. ustawień pomieszczeń oraz najczęściej popełnianych błędów

Ustawienia w pomieszczeniach ulegają zmianie, wchodząc do dziekanatu czy pokoju służbowego pracowników, student nie ma prawa widzieć tego co znajduje na monitorze komputera, ani mieć dostępu do dokumentów innych niż dotyczące jego osoby.

Pracownicy portierni w budynkach PWSZ w Elblągu (DS-y, Instytuty) mogą poprosić studenta o wylegitymowanie się dowodem osobistym, ale nie mogą zatrzymać, ani kserować tego dokumentu.

Incydenty

Bezpieczeństwo informacji to incydenty, które należy zgłaszać inspektorowi ochrony danych. Wymienione sytuacje są typowymi, ale wszystkie zdarzenia które wydają się podejrzanymi i które mogą zagrażać bezpieczeństwu danych osobowych należy zgłosić do IOD. Do typowych sytuacji zaliczyć można:

- a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
- b) dokumentacja jest niszczona bez użycia niszczarki,
- c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
- d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
- e) ustawienie monitorów pozwala na wgląd osób postronnych na dane osobowe,
- f) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz uczelni bez upoważnienia,
- g) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,
- h) telefoniczne próby wyłudzenia danych osobowych,
- i) kradzież komputerów lub CD, twarde dysków, nośniki cyfrowe z danymi osobowymi,
- j) maile zachęcające do ujawnienia identyfikatora i/lub hasła,
- k) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
- l) hasła do systemów przyklejone są w pobliżu komputera,
- m) inne