Załącznik
do zarządzenia nr 26/2023/2024
Dyrektora
Zespołu Szkolno-Przedszkolnego w Borowej
z dnia 20 października 2023

Procedura ochrony danych osobowych w ramach pracy zdalnej

I. Zakres podmiotowy procedury

1. Procedura określa zasady postępowania z danymi osobowymi w przypadku ich przetwarzania podczas pracy poza siedzibą pracodawcy.
2. Zakresem procedury objęci są pracownicy wykonujący pracę zdalną na podstawie:
   a) art. 67^{19} § 1 Kodeksu pracy (praca zdalna uzgodniona między pracownikiem a pracodawcą),
   b) art. 67^{19} § 3 Kodeksu pracy (obligatoryjna praca wykonywana na polecenie pracodawcy),
   c) art. 67^{19} § 6 Kodeksu pracy (obligatoryjna praca zdalna na wniosek pracownika).

II. Podstawowe pojęcia

1) dane osobowe – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizyczne, np. imię i nazwisko, numer identyfikacyjny (PESEL), adres zamieszkania, adres e-mail,
2) naruszenie ochrony danych osobowych – takie naruszenie bezpieczeństwa, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
3) pracownik wykonujący pracę zdalną – osoba zatrudniona na podstawie przepisów kodeksu pracy, w jeden ze sposobów określonych w art. 67^{19} § 1 Kodeksu pracy (w rozumieniu procedury nie jest pracownikiem wykonującym pracę zdalną osoba zatrudniona na podstawie umów cywilnoprawnych).

III. Obowiązki ogólne

1. Każdy pracownik wykonujący pracę zdalną jest zobowiązany do stosowania obowiązujących w zakładzie pracy wewnętrznych aktów dotyczących ochrony informacji i danych osobowych, a także procedur lub instrukcji dotyczących działania systemów informatycznych obowiązujących u pracodawcy.
2. Każdy pracownik ma obowiązek uczestniczenia w szkoleniach z zakresu ochrony danych osobowych, na które kieruje go pracodawca.
3. Każdy pracownik ma obowiązek zgłaszania wszelkich podejrzeń naruszeń ochrony danych osobowych. Każdy incydent należy zgłosić na adres iod@borowa.pl

4. Należy ograniczyć do niezbędnego minimum drukowanie dokumentacji zawierającej dane osobowe, a jeżeli taka konieczność zaistnieje, należy niszczyć wydruki po zakończeniu pracy z nimi.
5. Nie jest dopuszczalne korzystanie i zapisywanie na własnych nośnikach plików zawierających dane osobowe, których administratorem jest pracodawca, bez jego zgody i bez wcześniejszego zabezpieczenia przez pracodawcę.
6. Nie jest dopuszczalne umożliwianie dostępu do danych, poczty elektronicznej lub systemów informatycznych osobom nieuprawnionym, próbujących uzyskać dostęp drogą telefoniczną lub mailową, podającym się za przedstawicieli serwisu lub konkretnych instytucji, bez ich weryfikacji i potwierdzenia w zakładzie pracy takiego kontaktu.

IV. Obowiązki pracowników korzystających wyłącznie z poczty elektronicznej

Każdy pracownik korzystający z poczty elektronicznej jest zobowiązany do:

1) przechowywania loginu i hasła do poczty elektronicznej w bezpiecznym miejscu, niedostępnym dla osób nieuprawnionych, w tym domowników,
2) korzystania z poczty elektronicznej wyłącznie w celach służbowych,
3) archiwizowania korespondencji służbowej przy użyciu dedykowanych temu celowi narzędzi poczty elektronicznej,
4) nieprzesyłania korespondencji służbowej na jakąkolwiek prywatną skrzynką pocztową.

V. Obowiązki pracowników korzystających z poczty elektronicznej i systemów teleinformatycznych

Każdy pracownik korzystający z poczty elektronicznej i systemów teleinformatycznych jest zobowiązany do:

1) stosowania zasad określonych w pkt IV,
2) nieudostępniania danych dostępowych do systemów informatycznych osobom nieuprawnionym, w tym domownikom,
3) niepobierania danych osobowych z systemów informatycznych w celu innym niż służbowy,
4) pobierania i zapisywania tylko niezbędnych dokumentów.

VI. Obowiązki podczas spotkań zdalnych, wideokonferencji

1. Organizacja spotkań może nastąpić tylko przy użyciu dostarczonych przez pracodawcę rozwiązań informatycznych.
2. Podczas spotkań przebiegających z ujawnianiem wizerunków należy ograniczyć do minimum rejestrowanie spotkań.
3. W przypadku konieczności udostępniania konkretnych dokumentów podczas spotkań należy zamknąć używane wcześniej inne dokumenty, aplikacje, okna przeglądarek, aby udostępnić uczestnikom spotkania tylko i wyłącznie dedykowany dla nich plik.

4. Wszystkie pliki zapisywane w zespołach lub dedykowanej do tego przestrzeni w aplikacji do wideokonferencji należy cyklicznie przeglądać i usuwać po ustaniu ich przydatności.
5. Linki do wideokonferencji powinny być udostępniane tylko i wyłącznie uczestnikom spotkania, bezpiecznym kanałem komunikacji, zaproszenia powinny być kierowane wyłącznie na służbowe adresy e-mail.