

## **Procedura ochrony danych osobowych w ramach pracy zdalnej**

Działając na podstawie art. 67<sup>26</sup> Kodeksu Pracy, Pracodawca - Instytut Skrzynki - Instytut Dokumentacji, Rozwoju i Promocji Dziedzictwa Kulturowego i Kulinarnego, pl. Parkowy 1, 62-060 Skrzynki określa na potrzeby wykonywania pracy zdalnej niniejszą procedurę ochrony danych osobowych (dalej jako „Procedura”).

### **Postanowienia ogólne**

#### **§ 1**

1. Pracownik wykonujący pracę zdalną zobowiązany jest w jej trakcie do przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności z przepisami o ochronie danych osobowych, w tym przepisami Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych), zwanego dalej także „RODO”, oraz przepisami regulującymi ochronę danych osobowych u Pracodawcy, a także zgodnie z niniejszą Procedurą.
2. W ramach pracy zdalnej Pracownik zobowiązany jest do przetwarzania udostępnionych mu danych osobowych jedynie w celach związanych z zatrudnieniem u Pracodawcy i realizacją obowiązków służbowych.
3. Zabronione jest wykorzystywanie przez Pracownika udostępnionych mu danych osobowych w celach niezwiązanych z wykonywaniem zadań i obowiązków służbowych u Pracodawcy.

### **Zakres podmiotowy procedury**

#### **§ 2**

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<sup>19</sup> § 1 Kodeksu pracy (praca zdalna uzgodniona między pracownikiem a pracodawcą),
  - b) art. 67<sup>19</sup> § 3 Kodeksu pracy (obligatoryjna praca wykonywana na polecenie pracodawcy),
  - c) art. 67<sup>19</sup> § 6 Kodeksu pracy (obligatoryjna praca zdalna na wniosek pracownika).

## **Podstawowe pojęcia**

### **§ 3**

- 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<sup>19</sup> § 1 Kodeksu pracy (w rozumieniu procedury nie jest pracownikiem wykonującym pracę zdalną osoba zatrudniona na podstawie umów cywilnoprawnych).

### **§ 4**

#### **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 mail: kontakt@instytutskrzynki.pl lub telefonicznie; nr telefonu: 519 356 043.

#### **Bezpieczeństwo obszaru przetwarzania**

### **§ 5**

1. Pracownik jest zobowiązany do i odpowiedzialny za właściwe zabezpieczenie danych osobowych przetwarzanych przez niego w ramach pracy zdalnej, w szczególności zabezpieczenia dostępu do nich przed osobami postronnymi, zabezpieczenia ich przed utratą, zniszczeniem lub uszkodzeniem.
2. W ramach obowiązku określonego w ust. 1 powyżej Pracownik jest zobowiązany w szczególności do:
  - 1) Niekorzystania z otwartych, publicznych sieci WiFi, na przykład WiFi hotelowe, w galeriach handlowych lub hot-spot w kawiarniach,
  - 2) Nieudostępniania danych dostępowych do systemów informatycznych osobom nieuprawnionym, w tym domownikom, znajomym,
  - 3) Nieudostępniania służbowych urządzeń oraz danych osobowych osobom postronnym, w tym znajomym, dzieciom lub innym członkom rodziny,
  - 4) Nieudostępnianie 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.
- 5) Korzystania z poczty elektronicznej wyłącznie w celach służbowych,
  - 6) Nieprzesyłania korespondencji służbowej na jakąkolwiek prywatną skrzynką pocztową.
  - 7) Uniemożliwiania wglądu osobom postronnym w treści wyświetlane na ekranie sprzętu komputerowego, na przykład poprzez odpowiednie ustawienie ekranu.
  - 8) Stosowania polityki czystego ekranu, tj. blokowania sprzętu komputerowego przed każdorazowym oddaleniem się od stanowiska pracy (niezależnie od czasu oddalenia się) oraz ustawienia automatycznej blokady sprzętu/wygaszacza ekranu po 5 minutach,
  - 9) Wyłączania komputera służbowego po zakończeniu wykonywania pracy zdalnej
  - 10) Niepozostawiania służbowych dokumentów lub innych nośników informacji niezabezpieczonych, bez nadzoru, na widoku, dostępnych dla osób trzecich,
  - 11) Zachowanie zasady „czystego biurka” - w przypadku oddalania się ze stanowiska pracy zdalnej jak również po zakończeniu pracy zdalnej wszelkie dokumenty papierowe dotyczące spraw służbowych, w tym zawierające dane osobowe, winny być chowane do miejsca niedostępnego dla innych osób (np. szuflady lub szafy zamykanej na klucz),
  - 12) Niewykonywania służbowych telefonów lub wideokonferencji w towarzystwie innych osób, w tym domowników, współlokatorów,
  - 13) Nieużywania danych osobowych w celach lub w sytuacjach prywatnych niezwiązanych z wykonywaniem obowiązków pracowniczych,
  - 14) Niepobierania danych osobowych z systemów informatycznych w celu innym niż służbowy,
  - 15) Pobierania i zapisywania tylko niezbędnych dokumentów.
  - 16) Niezapisywanie na własnych nośnikach plików zawierających dane osobowe, których administratorem jest pracodawca, bez jego zgody.
  - 17) Ograniczenia do niezbędnego minimum drukowania dokumentacji zawierającej dane osobowe, a jeżeli taka konieczność zaistnieje, należy niszczyć wydruki po zakończeniu pracy z nimi za pomocą niszczarki. W przypadku braku niszczarki należy w bezpieczny sposób dostarczyć dokumenty do zakładu, w którym należy zniszczyć za pomocą niszczarki niepotrzebne wydruki.
  - 18) Zabronione jest wyrzucanie dokumentów dotyczących spraw służbowych, w tym zawierających dane osobowe, do domowych śmieci.

### **Obowiązki podczas spotkań zdalnych, wideokonferencji**

#### **§ 5**

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. Spotkanie można rejestrować tylko w sytuacji, gdy żaden uczestnik nie zgłosi sprzeciwu przez rozpoczęciem nagrywania.
4. W przypadku konieczności udostępniania konkretnych dokumentów podczas spotkań należy zamknąć używane wcześniej inne dokumenty, aplikacje, okna przeglądark, aby udostępnić uczestnikom spotkania tylko i wyłącznie dedykowany dla nich plik.
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.