COUNCIL OF EUROPE CONSEIL DE L'EUROPE

ZALECENIE CM/REC(2015) 5 KOMITETU MINISTRÓW DLA PAŃSTW CZŁONKOWSKICH NA TEMAT OCHRONY DANYCH OSOBOWYCH WYKORZYSTYWANYCH DLA CELÓW ZATRUDNIENIA

(Przyjęte przez Komitet Ministrów w dniu 1 kwietnia 2015 r. na 1124 spotkaniu Zastępców Ministrów).

Komitet Ministrów, na podstawie artykułu 15.b Statutu Rady Europy,

Zważywszy, że celem Rady Europy jest osiągnięcie większej jedności między jej członkami,

Świadomi wzrastającego wykorzystania nowych technologii oraz środków komunikacji elektronicznej w stosunkach pomiędzy pracodawcami i pracownikami, a także korzyści wynikających z tychże;

Uważając jednakże, że wykorzystywanie metod przetwarzania danych przez pracodawców powinno być kierowane przez zasady, stworzone tak aby zminimalizować jakiekolwiek ryzyko, które takie metody mogą powodować odnośnie praw oraz podstawowych wolności pracowników, w szczególności ich prawa do prywatności;

Uwzględniając przepisy Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 r. (dalej zwaną „Konwencją 108") oraz jej Dodatkowy Protokół dotyczący organów nadzorczych oraz między-granicznego przepływu danych z 8 listopada 2001 r., oraz chęć wyjaśnienia ich zastosowania w sektorze zatrudnienia;

Zauważając także, że interesy, które należy wziąć pod uwagę tworząc zasady dla sektora zatrudnienia mają charakter indywidualny lub zbiorowy, prywatny lub publiczny;

Uznając, że dane osobowe w dokumentach publicznych przechowywanych przez instytucje lub organy publiczne mogą być ujawnione przez instytucję lub organ zgodnie z prawem krajowym, któremu instytucja lub organ podlega, godząc w ten sposób dostęp do takich publicznych dokumentów z prawem do ochrony danych osobowych, zgodnie z zasadami niniejszej rekomendacji;

Będąc świadomym różnych tradycji, istniejących w państwach członkowskich w odniesieniu do regulacji różnych aspektów stosunku pracodawca-pracownik, a także zauważając, że prawo jest jedynie jednym ze środków regulujących ten stosunek;

Będąc świadomym międzynarodowych zmian, które wystąpiły w sektorze zatrudnienia oraz związanych z tym działań; w szczególności w związku ze zwiększającym się wykorzystaniem technologii informacyjno-komunikacyjnych (ICT) a także globalizacją zatrudnienia oraz usług;

Uznając, że w świetle takich zmian Rekomendacja Nm 89 (2) Komitetu Ministrów dla Państw Członkowskich w sprawie ochrony danych osobowych wykorzystywanych do celów zatrudnienia powinna być zmieniona, tak aby nadal zapewniała odpowiedni poziom ochrony dla jednostek w sektorze zatrudnienia;

Przypominając, że art. 8 Europejskiej Konwencji Praw Człowieka chroni prawo do życia prywatnego, włączając działania o charakterze zawodowym lub biznesowym, zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka;

Przywołując zastosowanie istniejących zasad przedstawionych w innych odpowiednich zaleceniach Rady Europy, w szczególności Rekomendacji CM/REC(2010)13 Komitetu Ministrów do Państw Członkowskich w sprawie ochrony jednostek w odniesieniu do automatycznego przetwarzania danych w kontekście profilowania, Rekomendacji R(97)5 w sprawie ochrony danych medycznych oraz Rekomendacji R(92)3 w sprawie testów genetycznych oraz prześwietlania dla celów ochrony zdrowia;

Przywołując „Wytyczne w sprawie ochrony jednostek w odniesieniu do zbierania oraz przetwarzania danych za pomocą środków wideonadzoru”, przyjęte przez Europejski Komitet ds. Współpracy Prawnej (CDCJ) Rady Europy w maju 2013 r., do którego odniesiono się w Rezolucji 1604(2008) Zgromadzenia Parlamentarnego Rady Europy w sprawie na nadzoru nad przestrzeniami publicznymi, które są szczególnie właściwe;

Przywołując Europejską Kartę Społeczną (ETS Nm. 163) w brzmieniu nadanym jej 3 maja 1996 r., a także Kodeks postępowania w odniesieniu do ochrony danych osobowych pracowników, przyjęty przez Międzynarodowe Biuro Pracy w 1997 r.;

Zaleca aby rządy państw członkowskich:

- zapewniły, aby zasady zawarte w załączniku do niniejszej rekomendacji, który zastępuje wspomnianą powyżej Rekomendacje (89)2, znalazły odzwierciedlenie w stosowaniu krajowego prawa ochrony danych w odniesieniu do sektora zatrudnienia, jak również w innych dziedzinach prawa, które wpływają na wykorzystanie danych osobowych dla celów zatrudnienia;
  w powyższym celu zapewniły, aby niniejsza Rekomendacja oraz jej załącznik zostały przedstawione organom utworzonym na podstawie krajowego ustawodawstwa o ochronie danych, które są właściwe do nadzorowania wdrożenia tego ustawodawstwa;
  promowały przyjmowanie oraz wdrażanie zasad zwartych w załączniku do niniejszej rekomendacji poprzez instrumenty towarzyszące takie jak regulaminy, tak aby zapewnić, że zasady są dobrze znane, rozumiane oraz stosowane przez wszystkie podmioty sektora zatrudnienia, włączając w to przedstawicieli zarówno pracodawców jak i pracowników, a także, że są brane pod uwagę w trakcie tworzenia oraz wykorzystywania systemów informatycznych w sektorze zatrudnienia.

Załącznik do Rekomendacji CM/REC (2015)5

Część I – Zasady ogólne

1. *Zakres*

1.1. Zasady przedstawione w niniejszej rekomendacji znajdują zastosowanie do jakiegokolwiek zbierania oraz przetwarzania danych osobowych dla celów zatrudnienia, zarówno w sektorze publicznym jak i prywatnym;

1.2. O ile prawo krajowe nie stanowi inaczej, zasady niniejszej rekomendacji stosuje się również do działań agencji zatrudnienia, zarówno w sektorze publicznym jak i prywatnym, które przetwarzają dane osobowe w celu umożliwienia zawarcia jednej lub więcej równoległych umów o pracę, włączając umowy o pracę w niepełnym wymiarze godzin, pomiędzy zainteresowanymi jednostkami oraz przyszłymi pracodawcami, lub w celu udzielenia pomocy pracodawcom w byciu zwolnionym od obowiązków wynikających z tych umów;

2. *Definicje*

Dla celów niniejszej rekomendacji:

„Dane osobowe” oznaczają każdą informację odnoszącą się do zidentyfikowanej lub możliwej do zidentyfikowania jednostki („osoba, której dane dotyczą”);

„Przetwarzanie danych” oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych, a w szczególności gromadzenie, przechowywanie, utrwalanie, zmianę, odzyskiwanie, ujawnianie, udostępnianie, usuwanie lub zniszczenie danych, lub przeprowadzanie logicznych lub/oraz arytmetycznych operacji na danych; tam gdzie nie wykorzystuje się automatycznego przetwarzania danych, przetwarzanie danych oznacza operację przeprowadzaną w ramach zbioru, zorganizowanego zgodnie z jakimikolwiek kryteriami, które pozwalają na wyszukanie danych osobowych;

„Systemy informacyjne” oznaczają każde urządzenie lub grupę połączonych lub powiązanych urządzeń, z których jedno lub więcej, zgodnie z programem, przetwarza w sposób automatyczny dane komputerowe, jak również dane komputerowe przechowywane, przetwarzane, odzyskiwane lub przechowywane przez nie w celu wykonywania operacji, korzystania, ochrony lub utrzymania;

„Cele związane z zatrudnieniem” dotyczą stosunków pomiędzy pracodawcami
a pracownikami, które odnoszą się do zatrudniania pracowników, wypełniania umowy o pracę, zarządzania, włączając w to zwolnienie z obowiązków ustanowionych przez prawo lub w umowach zbiorowych, jak również planowania oraz skutecznego prowadzenia organizacji oraz zakończenia stosunku pracy. Konsekwencje stosunku umownego mogą rozciągać się poza warunki umowy o pracę.

„Pracodawca” oznacza każdą osobę fizyczną lub prawną, instytucję publiczną lub agencję, która znajduje się w stosunku zatrudnienia z pracownikiem lub rozważa taki stosunek w odniesieniu do kandydata do pracy oraz ponosi prawną odpowiedzialność za przedsiębiorstwo lub przedstawicielstwo;

„Pracownik” oznacza każdą osobę zaangażowaną przez pracodawcą w ramach relacji zatrudnienia.

3. *Poszanowanie praw człowieka, godności oraz podstawowych wolności*

Poszanowanie ludzkiej godności, prywatności oraz ochrony danych osobowych powinno podlegać środkom ochronnym w ramach przetwarzania danych osobowych dla celów zatrudnienia, tak aby umożliwić swobodny rozwój osobowości pracowników oraz możliwości zawierania osobistych oraz społecznych związków w miejscu pracy.

4. *Stosowanie zasad przetwarzania danych*

4.1. Pracodawcy powinni minimalizować przetwarzanie danych osobowych jedynie do danych, które są niezbędne dla celu w określonym przypadku;

4.2. Pracodawcy powinni rozwinąć odpowiednie środki, tak aby zapewnić, że respektują w praktyce zasady oraz obowiązki dotyczące przetwarzania danych dla celów zatrudnienia. Na życzenie organu nadzorczego, pracodawcy powinni być także w stanie wykazać swoją zgodność z takimi zasadami oraz obowiązkami. Środki te powinny być dostosowane do ilości oraz charakteru przetwarzanych danych, rodzaju podejmowanej działalności, a także powinny również wziąć pod uwagę możliwe skutki dla podstawowych praw i wolności pracowników.

5. Zbieranie oraz przechowywanie danych

5.1. Pracodawcy powinni zbierać dane osobowe bezpośrednio od osoby, której dane dotyczą. Kiedy jest to konieczne oraz zgodne z prawem, aby przetwarzać dane zebrane od stron trzecich, na przykład w celu otrzymania referencji, osoba, której dane dotyczą powinna być zawczasu należycie poinformowana.

5.2. Dane osobowe zbierane przez pracodawców dla celów zatrudnienia powinny być odpowiednie i nie nadmierne, mając na uwadze charakter zatrudnienia jak również zmieniające się potrzeby informacyjne pracodawcy.

5.3. Pracodawcy powinni powstrzymać się od wymagania od nich lub zwracania się do pracownika lub osoby starającej się o pracę o dostęp do informacji, które ona lub on udostępnia innym przez Internet, w szczególności poprzez portale społecznościowe.

5.4. Dane dotyczące zdrowia mogą być zbierane jedynie dla celów ustanowionych w zasadzie 8.2. niniejszej Rekomendacji.

5.5. Przechowywanie danych osobowych dla celów zatrudnia jest dopuszczalne jedynie jeśli dane zostały zgromadzone w sposób zgodny z wymogami ustanowionymi w zasadach 4, 9, oraz od 14 do 20 niniejszej rekomendacji oraz tylko przez okres konieczny dla uzasadnionego celu przetwarzania. Dane te powinny być właściwe, odpowiednie oraz nienadmierne. W przypadku gdy przechowywane są dane ewaluacyjne dotyczące wyników lub potencjału pracowników, takie dane powinny być wykorzystane jedynie w celu oceniania umiejętności zawodowych.

6. ***Wewnętrzne wykorzystanie danych***

6.1. Dane osobowe zbierane do celów zatrudnienia, powinny być wykorzystywane przez pracodawców jedynie w tych celach.

6.1. Pracodawca powinien przyjąć polityki ochrony danych, zasady oraz/lub inne dokumenty dotyczące wewnętrznego wykorzystywania danych w zgodności z zasadami niniejszej rekomendacji.

6.3. W szczególnych okolicznościach, kiedy dane mają być przetwarzane dla celów zatrudnienia innych niż cel dla którego zostały pierwotnie zebrane, pracodawcy powinni podjąć odpowiednie środki w celu uniknięcia wykorzystania danych niezgodnie z przeznaczeniem dla innego celu oraz poinformować pracownika. W przypadku gdy istotne decyzje wpływające na pracownika mają zostać podjęte na podstawie przetwarzanych danych, pracownik powinien być poinformowany.

6.4. Bez uszczerbku dla zasady 8, w przypadku zmian korporacyjnych, połączeń oraz przejąć, należy poświęcić szczególną uwagę zasadom proporcjonalności oraz określenia celu przy dalszym wykorzystaniu danych. Jakakolwiek znacząca zmiana w przetwarzaniu powinna zostać zakomunikowana osobom, których to dotyczy.

7. *Komunikowanie danych oraz wykorzystanie technologii informacyjno-komunikacyjnych do celów reprezentowania pracowników*

7.1. Zgodnie z prawem krajowym oraz praktyką, lub na warunkach umów zbiorowych, dane osobowe mogą być zakomunikowane przedstawicielom pracowników, jednak jedynie w takich zakresie w jakim dane te są niezbędne do umożliwienia tym przedstawicielom reprezentowania interesów pracowników w odpowiedni sposób lub jeżeli takie dane są konieczne do wykonania oraz nadzoru nad obowiązkami ustanowionymi w umowach zbiorowych.

7.2. Zgodnie z prawem krajowym oraz praktyką, wykorzystanie systemów oraz technologii informacyjnych do komunikowania danych przedstawicielom pracowników powinno być przedmiotem odpowiedniej umowie zawierającej, z wyprzedzeniem, przejrzyste reguły określające ich wykorzystanie oraz środki ochronne w celu ochrony poufnej komunikacji, zgodnie z zasadą 10.

8. *Przekazywanie danych na zewnątrz*

8.1. Dane osobowe zbierane dla celów zatrudnienia powinny być przekazywane jedynie organom publicznym wykonującym swoje oficjalne funkcje i jedynie dla celu ich przeprowadzenia oraz jedynie w ramach ciążących na pracodawcy obowiązków prawnych lub w zgodzie z innymi przepisami prawa krajowego.

8.2. Przekazywanie danych osobowych organom publicznym dla celów innych niż wykonanie ich publicznych funkcji lub stronom innymi niż organy publiczne, włączając w to podmioty w tej samej grupie, może mieć miejsce jedynie:

a) w przypadku gdy przekazywanie jest niezbędne dla celów zatrudnienia, cele nie są niezgodne z celami dla których dane zostały pierwotnie zebrane oraz pracownicy lub jej lub jego przedstawiciele zostali o tym uprzednio poinformowani;

b) za wyraźną, dobrowolną oraz świadomą zgodą pracownika, którego to dotyczy;

c) jeżeli przekazanie jest dozwolone lub określone przez prawo krajowe
w szczególności gdzie to konieczne dla celów zwolnienia z obowiązków prawnych lub w zgodności z umowami zbiorowymi.

9. *Przetwarzanie danych wrażliwych*

9.1. Przetwarzanie danych osobowych o których mowa w artykule 6 Konwencji 108 jest możliwe jedynie w poszczególnych przypadkach, kiedy jest to nieuniknione dla rekrutacji na konkretne stanowisko lub wypełnienia obowiązków związanych
z umową o pracę w granicach ustanowionych w prawie krajowym oraz w zgodności
z odpowiednimi środkami ochronnymi, dopełniającymi te ustanowione w Konwencji 108 oraz w niniejszej rekomendacji. Odpowiednie środki ochronne powinny mieć za cel zapobieganie ryzykom, które przetwarzanie takich danych wrażliwych może stanowić dla interesów, praw oraz podstawowych wolności danego pracownika,
w szczególności ryzyku dyskryminacji. Przetwarzanie danych biometrycznych powinno być możliwe zgodnie z warunkami ustanowionymi w zasadzie 18 niniejszej rekomendacji.

9.2. Zgodnie z prawem krajowym, pracownikowi lub osobie starającej się o pracę mogą być zadane jedynie pytania dotyczące jej/jego stanu zdrowia oraz/lub mogą być zbadane pod kątem medycznym w celu:

a) określenia jej/jego zdolności dla obecnego lub przyszłego zatrudnienia;

b) wypełnienia wymogów profilaktyki zdrowotnej;

c) zagwarantowania odpowiedniej rehabilitacji lub zapewniania zgodności
z jakimikolwiek innymi wymogami środowiska pracy;

d) ochrony żywotnych interesów osoby, której dane dotyczą, lub innych pracowników i jednostek;

e) umożliwienia przyznania świadczeń socjalnych;

f) procedur sądowych.

9.3. Dane genetycznie nie mogą być przetwarzane, np. w celu określenia zdolności do pracy pracownika lub osoby starającej się o pracę, nawet za zgodą osoby, której dane dotyczą. Przetwarzanie danych genetycznych może być dopuszczone w wyjątkowych okolicznościach w szczególności aby uniknąć poważnego uszczerbku dla zdrowia osoby, której dane dotyczą lub stron trzecich i jedynie gdy jest to określone w prawie krajowym oraz przy zastosowaniu odpowiednich środków ochronnych.

9.4. Dane dotyczące zdrowia oraz, jeżeli ich przetwarzanie jest zgodne z prawem, dane genetyczne, powinny być zbierane jedynie od pracownika, jeżeli jest to określone przez prawo oraz przy zastosowaniu odpowiednich środków ochronnych.

9.5. Dane zdrowotne podlegające tajemnicy lekarskiej powinny być dostępne oraz przetwarzane jedynie przez personel, który jest związany takim obowiązkiem lub przez inne reguły zawodowej tajemnicy lub poufności. Dane takie muszą:

a) odnosić się bezpośrednio do zdolności danego pracownika do wykonywania jej lub jego obowiązków;
b) być konieczne do wspierania środków ochrony zdrowia pracownika;
c) być konieczne do zapobiegania wystąpienia ryzyk dla innych.

Jeżeli takie dane są komunikowane pracodawcom, przetwarzanie to powinno być przeprowadzone przez osobę z odpowiednim upoważnieniem, taką jak ktoś
z personelu administracyjnego lub odpowiedzialny za zdrowie lub bezpieczeństwo
w pracy a informacja powinna być zakomunikowana tylko jeżeli jest to nieuniknione dla podejmowania decyzji przez personel administracyjny oraz zgodnie z przepisami prawa krajowego.

9.6. Dane dotyczące zdrowia podlegające tajemnicy lekarskiej oraz, jeżeli ich przetwarzanie jest zgodne z prawem, dane genetyczne, tam gdzie to odpowiednie, powinny być przechowywane oddzielnie od innych kategorii danych osobowych przechowywanych przez

pracodawców. Powinny być przyjęte techniczne oraz organizacyjne środki bezpieczeństwa w celu zapobiegania temu aby osoby, które nie należą do służby medycznej pracodawcy miały dostęp do danych.

9.7. Dane medyczne dotyczące stron trzecich nie powinny być przetwarzane w żadnych okolicznościach jeżeli osoba, której dane dotyczą nie udzieli pełnej, jednoznacznej, swobodnej oraz świadomej zgody, lub jeżeli organ nadzorujący ochronę danych nie udzieli upoważnienia, lub jeżeli nie jest to wymagane na mocy prawa krajowego.

10. *Przejrzystość przetwarzania*

10.1. Informacja dotycząca danych osobowych przechowywanych przez pracodawców powinna być udostępniona bezpośrednio pracownikowi, którego to dotyczy lub za pośrednictwem jej lub jego przedstawicieli, lub przekazana za pomocą innych odpowiednich środków.

10.2. Pracodawcy powinni zapewnić pracownikom następujące informacje:

a) kategorie danych osobowych, które mają być przekazane oraz cele przetwarzania;
b) odbiorców, lub kategorie odbiorców danych osobowych;
c) środki, które są dostępne dla pracowników w celu wykorzystania praw ustanowionych; w zasadzie 11 niniejszej rekomendacji, bez uszczerbku dla bardziej korzystnych ustanowionych przez prawo krajowe lub w ich systemie prawnym;
d) jakiekolwiek inne informacje konieczne do zapewnienia uczciwego oraz zgodnego z prawem przetwarzania.

10.3 Szczególnie jasny i pełny opis musi być zapewniony wobec kategorii danych, które mogą być zbierane przy pomocy technologii informatycznych, włączając wideonadzór oraz ich możliwe wykorzystanie. Zasada ta znajduje również zastosowanie do szczególnych form przetwarzania określonych w Części II załącznika do niniejszej rekomendacji.

10.4 Informacja powinna być zapewniona w dostępnej formie oraz być aktualna.
W jakimkolwiek przypadku, taka informacja powinna być przekazana zanim pracownik przeprowadza daną czynność lub działanie oraz łatwo dostępna poprzez systemy informatyczne zwykle wykorzystywane przez pracownika.

11 *Prawo dostępu, poprawiania oraz sprzeciwu*

11.1 Pracownik powinien być w stanie uzyskać, na wniosek, w rozsądnym czasie oraz bez nadmiernej zwłoki potwierdzenie przetwarzania danych odnoszących się do niej lub do niego. Komunikat powinien mieć zrozumiałą formę, zawierać wszystkie informacje dotyczące źródła danych, jak również wszelkie inne informacje, do których podania administrator jest zobowiązany w celu zapewnienia przejrzystości przetwarzania, szczególnie informacje określone w zasadzie 10.

11.2 Pracownik powinien być uprawniony do tego, aby dotyczące jej lub jego dane zostały poprawione, zablokowane lub usunięte jeżeli są niedokładne oraz/lub jeżeli dane były przetwarzane niezgodnie z prawem lub zasadami ustanowionymi w niniejszej rekomendacji. Ona lub on powinni być również uprawnieni do wyrażenia sprzeciwu wobec przetwarzania danych osobowych jej lub jego dotyczących, chyba że przetwarzanie jest konieczne dla celów zatrudnienia lub w inny sposób przewidzianych przez prawo.

11.3 Prawo dostępu powinno być również zagwarantowane w przypadku danych ewaluacyjnych, włączając w to sytuację gdy takie dane dotyczą oceny wyników, produktywności lub zdolności pracownika, najpóźniej kiedy proces oceny został zakończony, bez uszczerbku do prawa obrony pracowników lub zaangażowanych stron trzecich. Chociaż takie dane nie mogą być bezpośrednio poprawione przez pracownika, czysto subiektywna ocena powinna być możliwa do zakwestionowania zgodnie z prawem krajowym.

11.4 Pracownik nie powinien być przedmiotem decyzji w sposób istotny wpływającej na nią lub na niego, podjętej jedynie na podstawie zautomatyzowanego przetwarzania danych, bez wzięcia pod uwagę jej lub jego opinii.

11.5 Pracownik powinien być również w stanie otrzymać, na prośbę, informację dotyczącą powodów przetwarzania danych, którego wyniki zostały do niego zastosowane.

11.6 Odstępstwa od praw określonych w akapitach 10, 11.1., 11.2., 11.4. oraz 11.5. mogą być dozwolone, jeżeli są określone przez prawo oraz stanowią niezbędny środek w społeczeństwie demokratycznym, w celu ochrony bezpieczeństwa państwa, bezpieczeństwa publicznego, ważnego interesu ekonomicznego oraz finansowego państwa lub zapobiegania oraz zwalczania przestępstw, ochrony osób, których dane dotyczą oraz praw i wolności innych.

11.7 Ponadto, w przypadku wewnętrznego dochodzenia przeprowadzanego przez pracodawcę, wykorzystanie praw o których mowa w akapitach 10, oraz od 11.1. do 11.5 może zostać odłożone do zamknięcia dochodzenia, jeżeli skorzystanie z tych praw mogłoby zagrozić dochodzeniu.

11.8 O ile przepisy prawa krajowego nie stanowią inaczej, pracownik powinien być uprawniony do wybrania oraz wyznaczenia osoby pomagającej jej lub mu w skorzystaniu z jej lub jego prawa dostępu, poprawienia lub wyrażenia sprzeciwu lub wykonania tych praw na jej lub jego rzecz.

11.9 Prawo krajowe powinno zawierać środek odwoławczy kiedy odmawia się prawa do dostępu lub poprawienia lub usunięcia jakichkolwiek danych.

10.3 *Bezpieczeństwo danych*

12.1. Pracodawcy lub podmioty, które mogą przetwarzać dane w ich imieniu, powinni zastosować adekwatne środki techniczne i organizacyjne na podstawie periodycznych przeglądów oceny ryzyka oraz polityk bezpieczeństwa organizacji, oraz uaktualniać je jeżeli to odpowiednie. Środki takie powinny być zaprojektowane tak, aby zapewnić bezpieczeństwo oraz poufność danych osobowych przetwarzanych dla celów zatrudnienia, przed przypadkową lub nieupoważnioną modyfikacją, stratą lub zniszczeniem danych osobowych, jak również przeciwko nieupoważnionemu dostępowi, rozpowszechnianiu lub ujawnieniu takich danych.

12.2. Zgodnie z prawem krajowym, pracodawcy powinni zapewnić odpowiednie bezpieczeństwo danych przy wykorzystaniu technologii informatycznych do jakiejkolwiek operacji przetwarzania danych osobowych do celów zatrudnienia, włączając ich przechowywanie.

12.2. Personel administracyjny, jak również jakakolwiek inna osoba zaangażowana w przetwarzanie danych, powinna być informowana o takich środkach oraz o potrzebie ich przestrzegania a także o potrzebie utrzymania poufności takich środków.

13. *Utrwalanie danych*

13.1. Dane osobowe nie powinny być przechowywane przez administratora przez okres dłuższy niż jest to uzasadnione przez cele zatrudnienia określone w zasadzie 2, lub jeśli jest to w interesie obecnego lub byłego pracownika.

13.2. Dane osobowe przekazane w związku z ubieganiem się o pracę powinny zwykle być niszczone po tym gdy stanie się jasne, że oferta zatrudnienia nie zostanie przedstawiona, lub jeżeli osoba ubiegająca się o zatrudnienie jej nie zaakceptuje. Jeżeli takie dane są przechowywane w związku z możliwą ofertą pracy, osoba powinna być poinformowana w odpowiednim czasie, a jej lub jego dane powinny być usunięte, jeżeli takie jest życzenie osoby.

13.3. W przypadku gdy kluczowe jest przechowywanie danych przekazanych w podaniu o pracę dla celów wniesienia lub odrzucenia powództwa, lub w jakimkolwiek innym uzasadnionym celu, dane powinny być przechowywane jedynie przez okres konieczny dla spełnienia tego celu.

13.4. Dane osobowe przetwarzane dla celów wewnętrznego dochodzenia przeprowadzanego przez pracodawcę, które nie doprowadziło do przyjęcia negatywnego środka wobec jakiegokolwiek pracownika, co do zasady, powinny być skasowane po rozsądnym czasie, bez uszczerbku dla prawa pracownika do dostępu, do momentu gdy takie usunięcie ma miejsce.

Część II – Poszczególne formy przetwarzania

14. *Wykorzystanie Internetu oraz komunikacji elektronicznej w miejscu pracy*

14.1 Pracodawcy powinni unikać nieuzasadnionego naruszenia prawa do prywatności pracownika. Zasada ta rozciąga się na wszystkie urządzenia techniczne oraz technologie informatyczne wykorzystywane przez pracownika. Osoba, której to dotyczy powinna być odpowiednio oraz systematycznie informowana poprzez zastosowanie odpowiedniej polityki prywatności zgodnie z zasadą 10 niniejszej rekomendacji. Podana informacja powinna być aktualna oraz powinna obejmować cel przetwarzania, okres utrwalania lub możliwości przywrócenia danych o ruchu oraz archwiziacje elektronicznych komunikatów służbowych.

14.2 W szczególności, w przypadku przetwarzania danych osobowych dotyczących stron internetowych lub intranetowych, do których mają dostęp pracownicy, powinno się preferować przyjęcie środków zapobiegawczych, takich jak filtry wykorzystania, które zapobiegają poszczególnym operacjom, a także stopniowanie możliwego monitorowania danych osobowych, preferując niezindywizualizowane losowe kontrole danych, które są zanonimizowane lub w jakiś sposób zagregowane.

14.3 Dostęp pracodawców do służbowej komunikacji elektronicznej pracowników, którzy zawczasu zostali poinformowani o takiej możliwości, może mieć miejsce tylko jeżeli to konieczne dla celów bezpieczeństwa lub z innych uzasadnionych powodów.
W przypadku nieobecności pracowników, pracodawcy powinni podjąć konieczne środki i przewidzieć odpowiednie procedury mające na celu umożliwienie dostępu do służbowej komunikacji elektronicznej tylko wtedy gdy taki dostęp jest konieczny ze służbowego punktu widzenia. Dostęp powinien być wykonany w możliwie jak najmniej inwazyjny sposób i jedynie po poinformowaniu danych pracowników.

14.4 Zawartość, wysyłanie oraz odbieranie prywatnej komunikacji elektronicznej w pracy nie powinno być monitorowane w żadnych okolicznościach.

14.5 W przypadku odejścia pracownika z organizacji, pracodawca powinien podjąć konieczne środki organizacyjne i techniczne w celu automatycznej dezaktywacji konta pracownika służącego do komunikacji elektronicznej. Jeżeli pracodawcy potrzebują odzyskać konta pracownika w celu skutecznego prowadzenia organizacji, powinni zrobić to przed jej lub jego odejściem oraz, jeżeli to wykonalne, w jej lub jego obecności.

15. *Systemy i technologie informacyjne do monitorowania pracowników, włączając wideonadzór*

15.1. Wprowadzenie oraz wykorzystanie technologii oraz systemów informacyjnych dla bezpośredniego oraz głównego celu monitorowania działań oraz zachowania pracownika nie powinno być dozwolone. Jeżeli ich wprowadzenie oraz wykorzystanie dla innych uzasadnionych celów, takich jak ochrona produkcji, zdrowia lub bezpieczeństwa lub zapewnienia skutecznego prowadzenia organizacji, skutkuje pośrednio możliwością monitorowania czynności pracowników, powinno być przedmiotem dodatkowych środków ochronnych, określonych w zasadzie 21, w szczególności konsultacji z przedstawicielami pracowników.

15.2. Systemy i technologie informacyjne, które pośrednio monitorują działania oraz zachowania pracowników powinny być szczególnie zaprojektowane oraz umieszczone, tak aby nie podważać ich praw podstawowych. Wykorzystanie wideonadzoru do monitorowania lokalizacji które są częścią najbardziej osobistej sfery życia pracowników nie jest dozwolone w żadnej sytuacji.

15.3. W przypadku sporu lub postępowania prawnego pracownicy powinny mieć możliwość otrzymania kopii jakichkolwiek nagrań, tam gdzie to odpowiednie oraz zgodnie z prawem krajowym. Przechowywanie nagrań powinno mieć wyznaczony limit czasowy.

16. *Urządzenia ujawniające miejsca pobytu pracownika*

16.1. Urządzenia ujawniające lokalizacje pracowników powinny być wprowadzane tylko jeżeli okaże się to konieczne do osiągnięcia uzasadnionego celu pracodawców a ich wykorzystanie nie powinno prowadzić do ciągłego monitorowania pracowników. Szczególnie, monitorowanie nie powinno być głównym celem, a jedynie pośrednią konsekwencją działań potrzebnych do ochrony produkcji, bezpieczeństwa oraz bezpieczeństwa pracy lub w celu zapewnienia skutecznego prowadzenia przedsiębiorstwa. Biorąc pod uwagę potencjał naruszenia podstawowych praw i

wolności danych osób poprzez wykorzystanie tych urządzeń, pracodawcy powinni zapewnić pracownikom wszystkie konieczne środki ochronne w odniesieniu do ich prawa do prywatności oraz do ochrony danych osobowych, włączając w to dodatkowe środki ochronne określone w zasadzie 21. Zgodnie z zasadami 4 oraz 5, pracodawcy powinni poświęcić specjalną uwagę celowi dla którego takie urządzenia są wykorzystywane oraz do zasad minimalizacji oraz proporcjonalności.

16.2. Pracodawcy powinni zapewnić odpowiednie procedury wewnętrzne dotyczące przetwarzania takich danych oraz powinni to zawczasu notyfikować osobom, których to dotyczy.

17. *Wewnętrzny mechanizm raportowania*

17.1 Jeżeli pracodawcy są zobligowani przez prawo lub wewnętrzne zasady do wdrożenia wewnętrznych systemów raportowania, takich jak telefoniczne linie informacyjne, powinni oni zabezpieczyć ochronę danych osobowych wszystkich zaangażowanych stron. W szczególności, pracodawcy powinni zapewnić poufność pracownika który raportuje o bezprawnym lub nieetycznym postępowaniu (np. whistleblower). Dane osobowe zaangażowanych stron powinny być wykorzystywane jedynie dla celu odpowiednich procedur wewnętrznych odnoszących się do zgłoszeń oraz zgodnie z wymogami prawa, lub wymogami następującego po tym postępowania sądowego.

17.2 W wyjątkowych okolicznościach, pracodawcy mogą umożliwić anonimowe raportowanie. Wewnętrzne dochodzenia nie powinny się opierać jedynie na podstawie anonimowego raportowania, za wyjątkiem sytuacji gdy jest należycie uzasadnione oraz odnosi się do poważnego naruszenia prawa krajowego.

18. *Dane biometryczne*

18.1. Zbieranie oraz dalsze przetwarzanie danych biometrycznych powinno być podejmowane jedynie wtedy gdy jest to konieczne do ochrony uzasadnionego interesu pracodawców, pracowników lub stron trzecich, jedynie jeżeli nie są dostępne inne mniej inwazyjne środki oraz jedynie jeżeli towarzyszą mu odpowiednie środki ochronne, obejmujące dodatkowe środki ochronne, określone w zasadzie 21.

18.2. Przetwarzanie danych biometrycznych powinno opierać się na naukowo uznanych metodach oraz podlegać ścisłym wymogom bezpieczeństwa oraz być proporcjonalne.

19. Testy psychologiczne, analizy oraz podobne procedury

19.1 Odwołanie się do testów psychologicznych, analiz oraz podobnych procedur przeprowadzanych przez wyszkolonych profesjonalistów, będących przedmiotem tajemnicy zawodowej, zaprojektowanych do oceny charakteru lub osobowości pracownika lub kandydata do pracy powinny być dozwolone jedynie jeżeli jest to uzasadnione oraz konieczne dla rodzaju czynności wykonywanych w pracy oraz jeżeli prawo krajowe ustanawia odpowiednie środki ochronne.

19.2 Pracownik lub kandydat do pracy powinien być poinformowany z wyprzedzeniem o użytku jaki będzie zrobiony z rezultatów tych badań, analiz oraz podobnych procedur oraz, następnie, o ich treści. Zasady 11.1 oraz 11.2 stosuje się odpowiednio.

20. ***Inne przetwarzanie stanowiące określone ryzyko dla praw pracownika***

20.1. Pracodawcy, lub gdzie ma to zastosowanie przetwarzający, powinni przeprowadzić analizę ryzyka potencjalnego wpływu zamierzonego przetwarzania danych na prawa oraz podstawowe wolności pracownika oraz zaprojektować operacje przetwarzania danych w taki sposób aby zapobiec lub przynajmniej zminimalizować ryzyko naruszenia tych praw oraz podstawowych wolności.

20.2. O ile prawo lub praktyka krajowa nie zapewnia innych odpowiednich środków ochronnych, powinno się dążyć do uzyskania zgody przedstawicieli pracowników przed wprowadzeniem lub adaptacją technologii informatycznych, tam gdzie analiza ujawnia ryzyka naruszenia praw oraz podstawowych wolności pracownika.

21. ***Dodatkowe środki ochronne***

Dla wszystkich poszczególnych form przetwarzania, przedstawionych w Części II niniejszej rekomendacji, pracodawcy powinni zapewnić w szczególności poszanowanie następujących środków ochronnych

a) poinformowania pracowników przed wprowadzeniem technologii oraz systemów informacyjnych umożliwiających monitorowanie ich działań. Przekazana informacja powinna być aktualna oraz powinna brać pod uwagę zasadę 10 niniejszej rekomendacji. Informacja ta powinna zawierać cel operacji, okresy utrwalenia lub przechowywania kopii zapasowej, jak również istnienie lub ich brak prawa dostępu oraz poprawiania oraz tego jak te prawa mogą być wykorzystane;

b) przyjęcia odpowiednich procedur wewnętrznych odnoszących się do przetwarzania tych danych oraz notyfikowania ich z wyprzedzeniem pracownikom;

c) konsultacji przedstawicieli pracowników w zgodzie z prawem lub praktyką krajową przed wprowadzeniem systemu monitorującego lub w przypadku gdy taki monitoring może się zmienić. Jeżeli procedura konsultacji ujawnia możliwość naruszenia prawa pracowników do poszanowania prywatności oraz godności ludzkiej, powinna być uzyskana zgoda przedstawicieli pracowników;

d) Konsultowania, zgodnie z prawem krajowym, krajowego organu nadzorczego w kwestii przetwarzania danych osobowych.