POLITYKA OCHRONY
DANYCH OSOBOWYCH

Administrator Danych Osobowych:

Spółka Lilla House sp. z o.o. z siedzibą w Łodzi

ul. Piotrkowska 276, 90-361 Łódź

KRS: 0000423090

WPROWADZENIE:

POLITYKA OCHRONY DANYCH OSOBOWYCH zwana dalej Polityką określa zasady przetwarzania danych osobowych, przy uwzględnieniu wymagań 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).

Niniejsza Polityka zawiera zbiór reguł i procedur obowiązujących przy przetwarzaniu danych osobowych w Spółce Lilla House sp. z o.o. Zastosowane rozwiązania i wdrożone procedury mają na celu zapewnienie właściwej ochrony przetwarzanych danych osobowych. Polityka zawiera również opis potencjalnych zagrożeń bezpieczeństwa przetwarzanych danych osobowych oraz sposoby reakcji w przypadku wystąpienia naruszenia bezpieczeństwa danych. W niniejszej polityce przewidziano również procedurę powierzenia danych osobowych innym podmiotom w celu realizacji zawartych umów głównych oraz przetwarzania danych osobowych powierzonych przez innych administratorów danych.

SŁOWNIK POJĘĆ:

1. **Polityka (Polityka bezpieczeństwa)** – należy przez to rozumieć niniejszą Politykę Ochrony Danych Osobowych;

2. **Dane osobowe** – informacje o osobie fizycznej, które umożliwiają jej bezpośrednie lub pośrednie zidentyfikowanie; w szczególności takie dane jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

3. **Dane wrażliwe** – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne lub dane biometryczne służące do jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej oraz dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa;

4. **Identyfikator użytkownika** - ciąg znaków składający się z liter, cyfr lub innych znaków pozwalający jednoznacznie zidentyfikować osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

5. **Hasło -** ciąg znaków składający się z liter, cyfr lub innych znaków znany jedynie osobie uprawnionej do korzystania z systemu informatycznego;

6. **Uwierzytelnianie —** działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby lub podmiotu;

7. **Administrator Danych Osobowych (ADO)** – Spółka Lilla House Spółka z ograniczoną odpowiedzialnością z siedzibą w Łodzi wpisana do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000423090,

8. **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora Danych Osobowych, do obowiązków której należy nadzór nas stosowaniem środków technicznych i organizacyjnych służących ochronie przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną;

9. **Administrator Systemu Informatycznego (ASI) –** osoba wyznaczona przez Administratora Danych Osobowych odpowiedzialna za prawidłowe funkcjonowanie sprzętu, oprogramowania oraz ich konserwację;

10. **Osoba upoważniona** – osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych, a udzielone przez ADO lub IOD

11. **Przetwarzanie danych** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

12. **System informatyczny**– zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych, a wykorzystywany przez Administratora Danych Osobowych;

13. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i stosowanie środków technicznych i organizacyjnych, które zapewniają ochronę danych przed ich nieuprawnionym przetwarzaniem, zniszczeniem, czy też dostępem do nich przez osoby nieuprawnione;

14. **Usuwanie danych** – zniszczenie danych osobowych lub ich modyfikacja, która trwale prowadzi do uniemożliwienia ustalenia tożsamości osoby, której dane dotyczą;

15. **Zgoda osoby, której dane dotyczą** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, przyzwala na przetwarzanie dotyczących jej danych osobowych, przy czym zgoda ta może zostać udzielona w formie oświadczenia lub wyraźnego działania potwierdzającego jej zgodę;

16. **Podmiot przetwarzający (Procesor)** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;

17. **Pracownik** - osoba zatrudniona przez Spółkę Lilla House sp. z o.o. na podstawie stosunku pracy;

18. **Współpracownik** – osoba świadcząca usługi na rzecz Spółki Lilla House sp. z o.o. w ramach innego stosunku prawnego niż umowa o pracę, w tym w oparciu o umowę zlecenia lub umowę o dzieło;

19. **Prezes Urzędu Ochrony Danych Osobowych (PUODO)** - organ powołany do spraw z zakresu ochrony danych osobowych;
20. **Rozliczalność** — właściwość zapewniająca, że działania na danych osobowych mogą być przypisane w sposób jednoznaczny tylko jednej osobie, a ponadto, właściwość zapewniająca możliwość udowodnienia realizacji praw osób, których dane osobowe są przetwarzane;
21. **Poufność danych** - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;
22. **Integralność danych** - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
23. **Integralność systemu** - nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

1. Postanowienia ogólne

1.1. Polityka jest dokumentem obowiązującym w Spółce Lilla House sp. z o.o. w zakresie wdrażania, przestrzegania i weryfikacji zasad ochrony danych osobowych.

1.2. Niniejszą politykę stosuje się do wszelkich operacji związanych z przetwarzaniem danych osobowych znajdujących się u ADO. Celem Polityki jest zapewnienie ochrony danych osobowych przed wszelakiego rodzaju zagrożeniami. Polityka bezpieczeństwa określa również tryb postępowania w przypadku ujawnienia naruszenia bezpieczeństwa przetwarzanych danych.

1.3. Wszystkie osoby dopuszczone do przetwarzania danych osobowych w ramach działalności Spółki Lilla House sp. z o.o., w tym Pracownicy i Współpracownicy, są zobowiązane zapoznać się z niniejszą Polityką oraz przestrzegać jej postanowień.

1.4. Naruszenie zasad wynikających z Polityki może stanowić podstawę wszczęcia postępowania dyscyplinarnego przeciwko Pracownikowi lub stanowić podstawę do rozwiązania umowy cywilnoprawnej w trybie natychmiastowym (o ile umowa tak stanowi).

1.5. Wszczęcie lub przeprowadzenie postępowania dyscyplinarnego przeciwko osobie naruszającej zasady wynikające z Polityki bezpieczeństwa nie wyklucza możliwości wszczęcia postępowania karnego oraz dochodzenia roszczeń z powództwa cywilnego.

1.6. Administrator Danych Osobowych sprawuje ogólny nadzór nad realizacją przepisów wynikających z ustawy o ochronie danych osobowych oraz 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).

1.7. W celu sprawowania nadzoru nad realizacją obowiązków wynikających z ustawy o ochronie danych osobowych oraz 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) ADO może powołać Inspektora Ochrony Danych. O powołaniu Inspektora Danych Osobowych

ADO zawiadamia Prezesa Urzędu Ochrony Danych Osobowych w terminie 14 dni od dnia jego ustanowienia.

1.8. W celu sprawowania nadzoru na prawidłowym funkcjonowaniem sprzętu i oprogramowania oraz jego konserwacji ADO może wyznaczyć Administratora Systemu Informatycznego.

1.9. W ramach działalności ADO dane osobowe są:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
- zbierane w konkretnych, wyraźnych i uzasadnionych celach oraz nieprzetwarzane dalej w sposób niezgodny z tymi celami,
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do realizacji celów, w których są przetwarzane,
- prawidłowe i w razie potrzeby uaktualniane, przy czym w sytuacji stwierdzenia nieprawidłowości danych należy podjąć wszelkie rozsądne działania, aby te dane osobowe zostały niezwłocznie usunięte lub sprostowane,
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane,
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

1.10. Przetwarzanie danych osobowych w ramach działalności ADO jest dopuszczalne w sytuacji, gdy wystąpi co najmniej jedna z poniższych okoliczności:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,

- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na ADO,
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
- kiedy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,
- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

1.11. Przetwarzanie Danych wrażliwych w ramach działalności ADO jest dopuszczalne w sytuacji, gdy wystąpi co najmniej jedna z poniższych okoliczności:

- osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach,
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez ADO lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy.

1.12. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, osoba taka jest informowana o:

- tożsamości i danych kontaktowych Administratora Danych Osobowych
- danych kontaktowych Inspektora Ochrony Danych, jeżeli zostanie powołany przez ADO,

- celach przetwarzania danych osobowych oraz podstawie prawnej ich przetwarzania;
- prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO, tj., gdy przetwarzanie danych odbywa się w celu realizacji prawnie uzasadnionych interesów administratora lub strony trzeciej;
- odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu,
- prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, przy czym zakres tej informacji dostosowany będzie każdorazowo do celów i sposobów przetwarzania;
- prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO, tj. wyrażenia zgody na przetwarzanie danych przez osobę, której dane dotyczą;
- prawie wniesienia skargi do organu nadzorczego,
- ustawowym lub umownym wymogu podania danych osobowych, lub o tym, czy podanie danych osobowych jest warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,

1.13. W przypadku zamiaru przetwarzania przez ADO danych osobowych w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem przekazuje on osobie, której dane dotyczą, informacje wskazane w pkt 1.12 Polityki, chyba że osoba, której dane dotyczą dysponuje już tymi informacjami. Postanowienia niniejszego pkt nie wyłączają konieczności uzyskania ponownej zgody na przetwarzanie danych osobowych, jeżeli dane te są przetwarzane na podstawie art. 6 ust. 1 lit. a) RODO.

1.14. W przypadku zbierania danych osobowych pozyskiwanych w sposób inny niż od osoby, której dane dotyczą, osoba taka jest informowana o:

- tożsamości i danych kontaktowych Administratora Danych Osobowych,

- danych kontaktowych Inspektora Ochrony Danych, jeżeli zostanie powołany przez ADO,
- celach przetwarzania danych osobowych oraz podstawie prawnej ich przetwarzania;
- kategorie odnośnych danych osobowych;
- odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
- okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu;
- prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO;
- prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych, przy czym zakres tej informacji dostosowany będzie każdorazowo do celów i sposobów przetwarzania;
- prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO;
- prawie wniesienia skargi do organu nadzorczego;
- źródle pochodzenia danych osobowych, ewentualnie czy pochodzą one ze źródeł publicznie dostępnych;

1.15. ADO może powierzyć innemu podmiotowi przetwarzanie danych osobowych w drodze umowy powierzenia, której wzór stanowi załącznik do niniejszej Polityki.

1.16. Każdej osobie, której dane osobowe są przetwarzane przez ADO, przysługuje prawo do uzyskania informacji czy przetwarzane są dane osobowe jej dotyczące, do uzyskania dostępu do nich, otrzymania kopii danych osobowych podlegających przetwarzaniu oraz do uzyskania informacji odnośnie:

- celów przetwarzania;
- kategorii odnośnych danych osobowych;
- odbiorców lub kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
- planowanego okresu przechowywania danych osobowych lub kryteriów ustalania tego okresu;
- prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane są przetwarzane, a także do wniesienia sprzeciwu wobec takiego przetwarzania;
- prawie wniesienia skargi do organu nadzorczego;
- dostępnych informacji o źródle danych, jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą;

1.17. Osoba, której dane dotyczą, ma prawo żądania od administratora sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych.

1.18. W przypadkach prawem przewidzianych, w szczególności, gdy przetwarzanie danych odbywa się w celach marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

1.19. Osoba, której dane dotyczą, ma prawo żądania od administratora usunięcia dotyczących jej danych osobowych, w sytuacji, gdy:
- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę udzieloną na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO i jednocześnie przetwarzanie danych nie odbywa się na innej podstawie prawnej uzasadniającej przetwarzanie;
- osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
- dane osobowe były przetwarzane niezgodnie z prawem;

– dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega ADO;
– dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego i dotyczą osoby poniżej 16 roku życia;

Żądanie usunięcia danych nie może być zrealizowane przez ADO w sytuacji, gdy przetwarzanie danych jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji, do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy obowiązujących przepisów albo do ustalenia, dochodzenia lub obrony roszczeń ADO.

1.19. Osoba, której dane dotyczą, ma prawo żądania od ADO ograniczenia przetwarzania:

-przez okres pozwalający administratorowi sprawdzić prawidłowość danych w sytuacji, gdy osoba ta kwestionuje prawidłowość jej danych osobowych przetwarzanych przez ADO,

- gdy przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

- gdy administrator nie potrzebuje już danych osobowych do celów w jakich zostały zebrane, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

1.20. W przypadku sprostowania, usunięcia lub ograniczeniu przetwarzania danych osobowych ADO informuje o tym fakcie każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

1.21. W przypadku, gdy przetwarzanie danych osoby, której dotyczą, odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO lub przetwarzanie danych odbywa się w sposób zautomatyzowany, jeżeli jednocześnie dane te są przetwarzane w formacie elektronicznym, osoba ta ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, a które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu

administratorowi, jak również może wnosić o bezpośrednie przekazanie tych danych innemu administratorowi, o ile jest to technicznie możliwe.

2 Obowiązki Administratora Danych Osobowych

2.1. Administrator Danych Osobowych zapewnia podstawy prawne do przetwarzania danych osobowych od chwili ich zebrania do chwili usunięcia, w szczególności poprzez stosowanie obowiązków informacyjnych oraz uzyskanie zgody na przetwarzanie danych osobowych osoby, której dane dotyczą, chyba że została spełniona inna przesłanka dopuszczająca przetwarzanie danych osobowych.

2.2. Administrator Danych Osobowych dba o prawidłowe przetwarzanie danych osobowych, w szczególności czuwa nad przestrzeganiem zasad aktualności danych osobowych, ich adekwatności oraz merytorycznej poprawności przetwarzanych w określonym celu danych osobowych.

2.3. Do obowiązków ADO należy ogólna kontrola nad tym, jakie dane osobowe, przez kogo i kiedy zostały wprowadzone, edytowane lub usunięte, co stanowi realizację obowiązku rozliczalności oraz dbałość o prawidłową realizację zasady czasowości, w szczególności poprzez zapewnienie usuwania danych osobowych po upływie niezbędnego czasu ich przetwarzania.

2.4. Administrator Danych Osobowych wykonuje czynności, które służą realizacji uprawnień osób, których dane osobowe są przetwarzane, w szczególności odnośnie sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia danych, czy też informowania o sprostowaniu, usunięcia lub ograniczeniu przetwarzania danych, a opisanych w pkt 1.17 – 1.21 niniejszej Polityki.

2.5. Administrator Danych Osobowych czuwa nad wdrożeniem procedur i środków bezpieczeństwa zapewniających prawidłowe przetwarzanie danych osobowych, a także ocenia skuteczność wdrożonej Polityki i środków bezpieczeństwa.

2.6. Administrator Danych Osobowych dokonuje analizy ryzyka wdrożonych procedur, środków bezpieczeństwa, czy też występujących u niego procesów przetwarzania danych osobowych.

2.7. Do obowiązków ADO należy prowadzenie i nadzór nad dokumentacją związaną z przetwarzaniem danych osobowych, co dotyczy w szczególności:

– Polityki Ochrony Danych Osobowych

- Rejestru Pracowników upoważnionych do przetwarzania danych,
- Rejestru Współpracowników upoważnionych do przetwarzania danych osobowych.

2.8. Upoważnienia do przetwarzania danych osobowych przez Pracowników i Współpracowników są nadawane i uchylane przez Administratora Danych Osobowych.

2.9. Nad wdrożeniem czynności związanych z zapoznawaniem się z przepisami i zasadami dotyczącymi ochrony danych osobowych oraz zagrożeniami związanymi z przetwarzaniem danych nadzór ogólny sprawuje ADO.

2.10. Administrator Danych Osobowych nadzoruje i zapewnia zgodne z prawem przekazywanie danych osobowych (udostępnianie i powierzanie).

2.11. Inspektora Ochrony Danych wyznacza ADO. Jednocześnie na ADO ciąży obowiązek zapewnienia środków i organizacyjnej odrębności Inspektorowi Ochrony Danych, które to są niezbędne do niezależnego wykonywania przez niego zadań.

2.12. Administrator Danych Osobowych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu Inspektora Ochrony Danych, w terminie 14 dni od dnia jego wyznaczenia.

2.13. Administrator Danych Osobowych zobowiązany jest podjąć niezbędne działania, a wynikające z niniejszej Polityki w przypadku stwierdzenia nieuprawnionego dostępu do danych osobowych lub naruszenia zabezpieczenia danych.

2.14. W przypadku naruszenia ochrony danych osobowych, Administrator Danych Osobowych, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, dokonuje zgłoszenia tego faktu do PUODO, chyba że występuje niewielkie prawdopodobieństwo, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Jednocześnie ADO zobowiązany jest do dokonania analizy okoliczności i przyczyn, które skutkowały naruszeniem ochrony danych osobowych, a następnie do przygotowania zaleceń i rekomendacji dotyczących eliminacji ryzyka ich wystąpienia w przyszłości.

3. Obowiązki Inspektora Ochrony Danych (IOD)

3.1 Inspektor Ochrony Danych jest powoływany na podstawie pisemnego oświadczenia Administratora Danych Osobowych.

3.2 Inspektor Ochrony Danych powinien posiadać odpowiednie kwalifikacje, a w szczególności posiadać fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych.

3.3 . Inspektor Ochrony Danych powinien być właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych oraz powinien mieć zapewniony dostęp do danych osobowych i operacji przetwarzania oraz do innych zasobów niezbędnych do wykonywania jego zadań, a także do zasobów niezbędnych do utrzymania jego wiedzy fachowej.

3.4 Do obowiązków Inspektora Ochrony Danych należy:

- udzielanie informacji o obowiązkach spoczywających na ADO oraz na Pracownikach i Współpracownikach, którzy przetwarzają dane osobowe na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie w sprawie zgodnego z prawem przetwarzania danych osobowych,
- monitorowanie przestrzegania przepisów prawa zawierających regulacje dotyczącą ochrony danych osobowych oraz przestrzegania Polityki ADO w dziedzinie ochrony danych osobowych, w tym podział obowiązków, podejmowanie działań zwiększających świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz uczestniczenie w przeprowadzanych audytach,
- prowadzenie Rejestru czynności przetwarzania danych osobowych oraz Rejestru kategorii czynności przetwarzania danych osobowych przetwarzanych w imieniu innego administratora,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych,
- w przypadku, gdy zachodzi ku temu przesłanka, pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

3.5 Niezależnie od obowiązków wymienionych w punkcie poprzednim, ADO może zlecić IOD przeprowadzenie analizy ryzyka w celu wdrożenia odpowiednich środków technicznych i organizacyjnych mających zapewnić przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa, a także w celu możliwości wykazania tejże okoliczności. Dokonując analizy ryzyka IOD bierze pod uwagę charakter przetwarzanych danych osobowych, zakres ich przetwarzania, cele i kontekst w jakich dane osobowe są przetwarzane, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

3.6 Inspektor Ochrony Danych Osobowych nie jest związany instrukcjami, które dotyczą wykonywania jego zadań. Nie może być odwoływany ani karany przez ADO ani Podmiot przetwarzający za wypełnianie swoich zadań. Inspektor Ochrony Danych podlega bezpośrednio najwyższemu kierownictwu ADO lub Podmiotu przetwarzającego.

3.7 Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

3.8 W przypadku braku powołania IOD, obowiązki opisane w niniejszym rozdziale wykonuje ADO.

4. Obowiązki Administratora Systemu Informatycznego (ASI)

4.1 ADO może wyznaczyć Administratora Systemu Informatycznego. Wyznaczenie ASI dokonane zostanie w formie pisemnej. ASI może zostać w każdym czasie odwołany przez ADO, jak również w każdym czasie może zostać wyznaczony inny ASI.

4.2 Do podstawowych obowiązków ASI należy:

- wdrożenie i utrzymanie środków szyfrowania danych osobowych, przetwarzanych w ramach systemu informatycznego ADO, poprzez zabezpieczenie urządzeń służących do przetwarzania danych osobowych (np. komputerów, laptopów, smartfonów),
- dokonanie odpowiedniej konfiguracji systemu informatycznego służącego do przetwarzania danych osobowych, która to ma zagwarantować zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych osobowych,

- zabezpieczenie serwerów systemu informatycznego służącego do przetwarzania danych osobowych, w tym zapewnienie możliwości szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie wystąpienia incydentu fizycznego lub technicznego,
- dokonywanie testów i ocen skuteczności zastosowanych środków technicznych mających zapewnić bezpieczeństwo przetwarzania danych osobowych przy użyciu systemu informatycznego,
- dokonanie instalacji, skonfigurowanie i usuwanie oprogramowania używanego w urządzeniach teleinformatycznych wykorzystywanych do przetwarzania danych osobowych,
- sprawowanie nadzoru nad pracami podmiotów zewnętrznych, które dokonują napraw, konserwacji, itp. systemów informatycznych służących do przetwarzania danych osobowych,
- nadawanie, zmiana, pozbawianie i blokowanie Identyfikatorów i Haseł oraz uprawnień do korzystania z programów osobom przetwarzającym dane osobowe,
- sporządzanie kopii bezpieczeństwa nośników zawierających dane osobowe,
- podejmowanie działań mających na celu wykrycie naruszeń bezpieczeństwa w systemie zabezpieczeń systemu informatycznego, który służy do przetwarzania danych osobowych,
- świadczenie pomocy technicznej w zakresie obsługi oprogramowania i urządzeń używanych w ramach systemu informatycznego służącego do przetwarzania danych osobowych w ADO,
- zabezpieczenie haseł ASI i zapewnienie ADO dostępu do nich w sytuacjach wyższej konieczności / natury siły wyższej / niezdolności ASI do użycia haseł,
- określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych,
- nadzór nad przestrzeganiem procedur rozpoczęcia, zawieszenia i zakończenia pracy użytkowników systemu, oraz prowadzenie szkoleń dla użytkowników systemu,
- udział w postępowaniu wyjaśniającym związanym z zaistnieniem naruszenia danych osobowych w systemie,
- ograniczanie możliwości instalowania oprogramowania na stacjach roboczych przez osoby nieupoważnione,
- przeprowadzanie szkoleń użytkowników w zakresie procedur i instrukcji zapewniających ochronę danych osobowych w systemie.

4.3 Niezależnie od powyższych obowiązków ASI jest zobowiązany do ewidencjonowania czynności wykonywanych w systemie informatycznym

służącym do przetwarzania danych osobowych oraz do prowadzenia ewidencji urządzeń i nośników, służących do przetwarzania danych osobowych.

4.4 Przy wykonywaniu obowiązków ASI zobowiązany jest stosować się do poleceń ADO oraz IOD. W przypadku, gdyby wydane polecenie uniemożliwiało, lub utrudniało realizację obowiązków, w tym było sprzeczne z Polityką, ASI zobowiązany jest pisemnie poinformować o tym ADO.

5. Powierzanie przetwarzania danych osobowych

5.1 ADO może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie przetwarzanie danych. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik do Polityki.

5.2 Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie, oraz zobowiązany jest przed rozpoczęciem przetwarzania danych podjąć środki, które zapewniają odpowiednią ochronę praw osób, których dane dotyczą.

5.3 Podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody ADO. W przypadku udzielenia ogólnej pisemnej zgody Podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających.

5.4 Spółka Lilla House sp. z o.o. w charakterze podmiotu przetwarzającego (procesora) może przyjąć do przetwarzania dane osobowe powierzone przez odrębnych ADO. Powierzenie przetwarzania danych osobowych odbywa się na podstawie umowy, która określa w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

6. Upoważnieni do przetwarzania danych osobowych

6.1 Do przetwarzania danych osobowych mogą być dopuszczone jedynie osoby posiadające odpowiednie pisemne upoważnienie nadane przez ADO, które zapoznały się z Polityką. Upoważnienie jest udzielane indywidualnie każdej osobie uprawnionej do przetwarzania danych osobowych.

6.2 Nadanie upoważnienia do przetwarzania danych osobowych musi nastąpić przed rozpoczęciem przetwarzania danych osobowych przez osobę upoważnioną.

6.3 Przetwarzanie danych osobowych przez osoby Upoważnione dobywa się wyłącznie na polecenie ADO.

6.4 Osoba, której ma zostać udzielone upoważnienie składa na piśmie oświadczenie o zachowaniu poufności, którego treść kształtowana jest w zależności od zakresu obowiązków danej osoby. Osoba upoważniona do przetwarzania danych osobowych, pod groźbą sankcji dyscyplinarnych lub uznania za naruszenie umowy cywilnoprawnej obowiązującej pomiędzy stronami tej umowy, ma obowiązek zachowania tajemnicy o przetwarzanych danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia lub współpracy.

6.5 Udzielone upoważnienie może zostać w każdym czasie odwołane przez ADO.

6.6 Wykaz osób upoważnionych do przetwarzania danych osobowych prowadzi ADO. Prowadzenie powyższego rejestru może zostać powierzone IOD.

6.7 Każda osoba, przed dopuszczeniem go do przetwarzania danych osobowych musi być zapoznana z przepisami dotyczącymi ochrony danych osobowych oraz Polityką.

6.8 Upoważnieni są w szczególności zobowiązani do:

- bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych, określonych w obowiązujących przepisach prawa oraz niniejszej Polityce,
- zabezpieczania wszelkich nośników zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce,
- nieudzielania żadnych informacji o przetwarzanych danych osobowych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione,
- niezwłocznego zawiadomienia IOD i ADO o wszelkich przypadkach naruszenia bezpieczeństwa przetwarzanych danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

7. Udostępnianie danych osobowych

7.1 Udostępnianiem danych osobowych są wszelkie działania umożliwiające innym niż ADO podmiotom zapoznanie się z danymi osobowymi przetwarzanymi, z wyłączeniem opisanych wcześniej powierzeń.

7.2 Udostępnianie nie odnosi się do Pracowników i Współpracowników, który działają na podstawie udzielonych upoważnień.

7.3 Udostępnianie danych osobowych może mieć charakter odpłatny lub nieodpłatny.

7.4 Udostępnianie danych osobowych może być dokonane w formie ustnej, pisemnej, za pomocą powszechnych środków przekazu, poprzez sieć komputerową itd.

7.5 Udostępnianie danych osobowych odbywa się wyłącznie za zgodą osoby, której dane dotyczą, albo na podstawie obowiązującego prawa.

8. Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych

8.1 Naruszeniem bezpieczeństwa danych osobowych są zdarzenia polegające na:

- włamaniu do systemu, podsłuchu, kradzieży danych lub sprzętu,
- świadomej bądź nieumyślnej modyfikacji danych osobowych,
- włamaniu do systemu informatycznego,
- wyciek informacji,
- ujawnieniu danych osobowych osobom nieuprawnionym,
- działaniu programów zawierających wirusy,
- uszkodzeniu oprogramowania,
- awarii serwera bądź wykorzystywanego przy przetwarzaniu danych osobowych sprzętu komputerowego i elektronicznego,
- niewłaściwym zabezpieczeniu pomieszczeń, urządzeń i dokumentów,
- nieprzestrzeganiu zasad ochrony danych osobowych przez osoby uprawnione do przetwarzania danych osobowych,
- wystąpieniu zdarzenia losowego,
- innych niż wyżej opisane zdarzeniach skutkujących utratą danych osobowych lub wejściem w ich posiadanie osób nieuprawnionych.

8.2 W przypadku stwierdzenia faktu nieuprawnionego przetwarzania, ujawnienia lub nienależytego zabezpieczenia danych osobowych oraz w przypadku stwierdzenia

istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia danych osobowych, każdy Pracownik bądź Współpracownik zobowiązany jest niezwłocznie poinformować o tym zdarzeniu IOD lub ADO.

8.3 W przypadku stwierdzenia naruszenia zasad ochrony danych osobowych, IOD lub ADO niezwłocznie:

- informuje osobę zgłaszającą o dalszym trybie postępowania i poleca jej podjęcie odpowiednich czynności zmierzających do wyeliminowania podobnych zagrożeń w przyszłości,
- podejmuje czynności pozwalające w miarę możliwości przywrócić stan zgodny z zasadami ochrony danych osobowych,
- ustala czas trwania oraz charakter zaistniałego naruszenia, oraz o ile to możliwe kategorie i przybliżoną liczbę osób, których dane zostały naruszone, a także kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- ustala możliwe konsekwencje naruszenia ochrony danych osobowych,
- zgłasza naruszenie, w ciągu 72 godzin (o ile to możliwe) do PUODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych,
- w razie konieczności inicjuje działania dyscyplinarne,
- dokumentuje prowadzone postępowanie w rejestrze naruszeń bezpieczeństwa danych osobowych,

8.4 Zgłoszenie naruszenia ochrony danych do PUODO zawiera:

- opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać niezbędne informacje,
- opis możliwych konsekwencji zaistniałego naruszenia ochrony danych osobowych,
- opis środków zastosowanych lub proponowanych przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych w przyszłości, w tym

w stosownych przypadkach opis środków zastosowanych lub proponowanych w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

8.5 Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie nie jest wymagane, gdy:

- ADO wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
- ADO zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
- wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku ADO wydaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

8.6 W przypadku przetwarzania danych osobowych w charakterze Procesora, Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

II PROCEDURY

1. PROCEDURA SPRAWOWANIA KONTROLI DOSTĘPU DO SYSTEM INFORMATYCZNEGO

1. Przy wykorzystywaniu systemu informatycznego do przetwarzania danych osobowych stosuje się mechanizmy kontrolujące dostęp do tych danych.
2. W sytuacji, gdy dostęp do przetwarzanych w systemie informatycznym danych osobowych posiada dwie lub więcej osób, należy zapewnić:

a. odrębny identyfikator dla każdego użytkownika tego systemu,

b. zabezpieczenie danych poprzez umożliwienie dostępu do nich wyłącznie po wprowadzeniu identyfikatora i podaniu hasła.

3. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, nie może być przydzielony innej osobie.

4. Systemu informatyczny służący do przetwarzania danych osobowych, przed rozpoczęciem przetwarzania danych osobowych, należy zabezpieczyć przed:

a. działaniem złośliwego oprogramowania, które mogłoby uzyskać nieuprawniony dostęp do systemu informatycznego,

b. utratą danych spowodowaną awarią, w szczególności awarią zasilania lub innymi zakłóceniami w sieci zasilającej.

2. PROCEDURA HASEŁ

1. Jeśli uwierzytelnienie użytkownika w systemie informatycznym służącym do przetwarzania danych osobowych następuje przy użyciu hasła, hasło powinno składać się z co najmniej 8 znaków, w tym małych i wielkich liter oraz cyfr lub znaków specjalnych.
2. Zabrania się użytkownikom ujawniania lub przekazywania przypisanego im hasła innym osobom.
3. Zabrania się przechowywania hasła w miejscach dostępnych dla innych osób niż osoba, dla której przypisane jest hasło.

3. PROCEDURA OCHRONY PRZED NIEPORZĄDANYM OPROGRAMOWANIEM

1. System informatyczny służący do przetwarzania danych osobowych chroniony jest przez oprogramowanie antywirusowe, którego zadaniem jest uniemożliwienie uzyskania nieuprawnionego dostępu do przetwarzanych danych osobowych.
2. W każdym urządzeniu wyposażonym w dostęp do sieci internetowej, musi być zainstalowanie oprogramowanie antywirusowe.

3. Pliki wczytywane do urządzenia, w tym także wiadomości e-mail, podlegają uprzedniemu sprawdzeniu przez oprogramowanie antywirusowe.
4. Zabrania się wyłączania programów antywirusowych.
5. Oprogramowanie antywirusowe musi być regularnie aktualizowane.
6. Nadzór nad zapewnieniem ochrony antywirusowej, w szczególności nad zakupem odpowiedniej ilości licencji oraz aktualizacji oprogramowania sprawuje ASI, a w przypadku braku jego powołania - ADO.

4. PROCEDURA SPORZĄDZANIA EWIDENCJI URZĄDZEŃ I NOŚNIKÓW DANYCH ORAZ ICH USUWANIA

1. Każde urządzenie i nośnik służący do przetwarzania danych powinien zostać oznaczony indywidualnym numerem.
2. Należy sporządzić pisemny wykaz wszystkich urządzeń i nośników służących do przetwarzania danych osobowych zawierający ich oznaczenie oraz lokalizację lub dane osoby używającej urządzenie lub nośnik.
3. Przed wprowadzeniem do używania nowych urządzeń i nośników służących do przetwarzania danych osobowych, należy je odpowiednio zewidencjonować.
4. Przed usunięciem nośnika lub urządzenia należy trwale (najlepiej z wykorzystaniem odpowiedniego oprogramowania lub przy wykorzystaniu procedury nadpisania) wykasować znajdujące się na nim dane.
5. W przypadku braku możliwości trwałego usunięcia danych z nośnika lub urządzenia, które służyło do przetwarzania danych osobowych, przed jego usunięciem należy dokonać jego fizycznego zniszczenia, które uniemożliwi odczytanie danych zgromadzonych na nośniku lub urządzeniu.
6. Po usunięciu urządzenia lub nośnika służącego do przetwarzania danych osobowych, należy uczynić odpowiednią wzmiankę w wykazie urządzeń i nośników.

5. PROCEDURA ZABEZPIECZENIA KOPII ZAPASOWYCH

1. Należy regularnie wykonywać kopie zapasowe danych osobowych przetwarzanych w systemie informatycznym.
2. Kopie zapasowe danych osobowych w systemie informatycznym wykonuje ASI, a w przypadku braku jego powołania osoba wyznaczona przez ADO.
3. Wykonane kopie zapasowe należy przechowywać się w miejscach uniemożliwiających dostęp osób niepowołanych oraz w sposób uniemożliwiający ich nieuprawnioną modyfikację, uszkodzenie, zniszczenie.
4. Nośniki zawierające wykonane zapasowe przechowuje się w odrębnej lokalizacji względem oryginału zabezpieczonych danych.

6. PROCEDURA KORZYSTANIA Z SIECI INTERNETOWEJ ORAZ POCZTY INTERNETOWEJ

1. Korzystanie z sieci internetowej jest możliwe jedynie w celu wykonywania obowiązków służbowych.
2. Podczas korzystania z przeglądarki internetowej zabrania się z korzystania z opcji autouzupełniania formularzy i zapamiętywania haseł.
3. Zabrania się uruchamiania pobranych z sieci internetowej plików z pominięciem skanowania ich przez program antywirusowy lub oznaczonych przez ten program jako niebezpieczne lub potencjalnie niebezpieczne.
4. Nie należy otwierać załączników (plików) w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę bez uprzedniej weryfikacji tych załączników przez oprogramowanie antywirusowe.
5. W przypadku stwierdzenia faktu pojawienia się szkodliwego oprogramowania lub stwierdzenia nieprawidłowości w funkcjonowaniu systemu informatycznego, należy niezwłocznie powiadomić o tym fakcie ASI lub ADO.
6. Zabrania się przesyłania danych osobowych przy użyciu nieszyfrowanych stron internetowych. W tym celu przed rozpoczęciem przesłania tych danych, należy sprawdzić czy w pasku adresu strony internetowej widoczna jest informacja o odpowiednim zabezpieczeniu (zielona kłódka, protokół https).
7. Zabrania się przesyłania danych osobowych do krajów spoza EOG bez uzyskania uprzednio zgody ADO.
8. Przed wysłaniem wiadomości zawierającej dane osobowe należy zweryfikować poprawność adresu e-mail adresata.
9. Podczas rozsyłania korespondencji wielu adresatom należy używać funkcji UDW, aby uniemożliwić wgląd w adresy e-mail innych odbiorców wiadomości.
10. W przypadku przesyłania danych osobowych za pośrednictwem poczty elektronicznej, należy wykorzystywać mechanizmy zabezpieczające plik zawierający dane osobowe (np. poprzez pakowanie i zabezpieczanie hasłem wysyłanych plików lub szyfrowanie w inny sposób). W takim przypadku hasło dostępowe do pliku powinno zostać udostępnione innym środkiem komunikacji (np. poprzez wiadomość SMS).

7. PROCEDURA KORZYSTANIA Z KOMPUTERA STACJONARNEGO

1. Przed rozpoczęciem z korzystania z komputera stacjonarnego wykorzystywanego do przetwarzania danych osobowych należy upewnić się, że ustawienie monitora uniemożliwia podgląd wyświetlanych danych osobom nieuprawnionym.
2. Przed każdorazowym rozpoczęciem z korzystania z komputera stacjonarnego wykorzystywanego w celu przetwarzania danych osobowych należy sprawdzić, czy nie występują oznaki fizycznego naruszenia zabezpieczeń, a także czy osoba

nieuprawniona nie usiłowała zalogować się do systemu informatycznego służącego do przetwarzania danych osobowych.

3. Przystępując do pracy z komputerem stacjonarnym wykorzystywanym do przetwarzania danych osobowych, osoba upoważniona zobowiązana jest wprowadzić swój identyfikator i hasło dostępu.
4. Zabrania się wykonywania jakichkolwiek czynności w systemie informatycznym służącym do przetwarzania danych osobowych przy wykorzystaniu identyfikatora lub hasła innej osoby upoważnionej.
5. W przypadku konieczności przerwania pracy na komputerze stacjonarnym służącym do przetwarzania danych osobowych na czas dłuższy niż 3 minuty lub zakończenia pracy, należy dokonać wylogowania.
6. Na ekranie komputera stacjonarnego należy zainstalować wygaszacz ekranu z opcją zabezpieczenia hasłem.
7. Zabrania się wynoszenia komputerów stacjonarnych z lokalizacji ADO.

8. PROCEDURA KORZYSTANIA Z URZĄDZEŃ PRZENOŚNYCH

1. Przed rozpoczęciem z korzystania z urządzeń przenośnych wykorzystywanych do przetwarzania danych osobowych należy upewnić się, że ustawienie wyświetlacza lub monitora uniemożliwia podgląd wyświetlanych danych osobom nieuprawnionym.
2. Przed każdorazowym rozpoczęciem z korzystania z urządzenia przenośnego wykorzystywanego w celu przetwarzania danych osobowych należy sprawdzić, czy nie występują oznaki fizycznego naruszenia zabezpieczeń, a także czy osoba nieuprawniona nie usiłowała zalogować się do systemu informatycznego służącego do przetwarzania danych osobowych.
3. Przystępując do pracy z urządzeniem służącym do przetwarzania danych osobowych, osoba upoważniona jest zobowiązana wprowadzić swój identyfikator i/lub hasło dostępu lub odblokować urządzenie przy użyciu danych biometrycznych.
4. Zabrania się wykonywania jakichkolwiek czynności w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora, hasła dostępu lub danych biometrycznych innej osoby upoważnionej.
5. W przypadku konieczności przerwania lub zakończenia pracy na urządzeniu przenośnym służącym do przetwarzania danych osobowych, należy dokonać wylogowania.
6. Komputery przenośne można wynosić z obszaru przetwarzania danych osobowych tylko po uzyskaniu uprzedniej zgody ADO. Komputer powinien być wyposażony

w oprogramowanie szyfrujące uniemożliwiające dostęp do danych w przypadku jego utraty.

7. Osoba, która użytkuje urządzenie przenośne służące do przetwarzania danych osobowych, zobowiązana jest zabezpieczyć je przed kradzieżą, ponadto powinna zachować szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza lokalizacją ADO.
8. Zabrania się korzystania z otwartych sieci internetowych przy użyciu urządzeń przenośnych służących do przetwarzania danych osobowych.
9. Zabrania się wywożenia urządzeń przenośnych służących do przetwarzania danych osobowych do krajów spoza EOG bez uzyskania uprzedniej zgody ADO.

9. PROCEDURA PRZETWARZANIA DANYCH OSOBOWYCH W FORMIE PAPIEROWEJ

1. Przetwarzane w formie papierowej dane osobowe mogą znajdować się na biurkach lub stołach tylko przez czas niezbędny do dokonania czynności służbowych. Po zakończeniu przetwarzania danych osobowych w formie papierowej dokumenty należy odłożyć do specjalnie wyznaczonych szaf.
2. Nie wolno pozostawiać dokumentów bez nadzoru.
3. Zbędne wydruki i inne dokumenty, zawierające dane osobowe, powinny być zniszczone w niszczarce dokumentów.
4. Za prawidłowe zniszczenie zbędnych dokumentów papierowych, zawierających dane osobowe, odpowiada osoba, która te dane przetwarzała.

10. POSTANOWIENIA KOŃCOWE

1. Polityka jest dokumentem wewnętrznym opracowanym dla Spółki i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

2. Do spraw nieuregulowanych w niniejszej Polityce stosuje się przepisy 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) oraz obowiązującej Ustawy o ochronie danych osobowych, a także wydanych na jej podstawie aktów wykonawczych, oraz inne obowiązujące przepisy obejmujące swoim zakresem problematykę ochrony danych osobowych.

3. Polityka nie wyłącza stosowania dodatkowo innych procedur dotyczących zabezpieczenia danych zgodnie z obowiązującymi przepisami.

4. Wobec osoby, która w przypadku naruszenia zasad przetwarzania danych osobowych określonych w niniejszej Polityce lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, możliwe będzie wszczęcie postępowania dyscyplinarnego, a przypadku współpracowników mogą zostać podjęte kroki prawne zmierzające do naprawienia wyrządzonej szkody.