

POLITYKA OCHRONY DANYCH OSOBOWYCH

PODWAWELSKA SPÓŁDZIELNIA SPOŻYWCÓW

Kraków
maj 2018

1. Podstawa prawna

- 1.1. Niniejszą Politykę ochrony danych osobowych w PODWAWELSKIEJ SPÓŁDZIELNI SPOŻYWCÓW ustanawia się dążąc do spełniania wymogu rozliczalności, na podstawie art. 5 ust. 2 w związku z art. 5 ust. 1 lit. c., d. oraz e., jak również w związku z art. 6 ust 1 lit. f., art. 15-21, art. 24 ust. 1, art. 33 oraz art. 35-37 RODO, a także biorąc pod uwagę dokumenty wydane przez „Grupę Roboczą art. 29” – a zwłaszcza:
 - 1.1.1. Guidelines on transparency under Regulation 2016/679,
 - 1.1.2. Guidelines on Personal data breach notification under Regulation 2016/679,
 - 1.1.3. Guidelines on Consent under Regulation 2016/679,
 - 1.1.4. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,
 - 1.1.5. Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” dla celów rozporządzenia 2016/679,
 - 1.1.6. Wytyczne dotyczące inspektorów ochrony danych ('DPO'),
 - 1.1.7. Opinię 2/12017 na temat przetwarzania danych w miejscu pracy.

2. Definicje

Ilekcioć w dokumentacji przetwarzania danych osobowych obowiązującej w PODWAWELSKIEJ SPÓŁDZIELNI SPOŻYWCÓW pojawiają się podane niżej sformułowania należy nadawać im podane niżej znaczenie (chyba, że dany dokument wprost wskazuje coś przeciwnego):

- 2.1. Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego 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.
- 2.2. Przetwarzanie danych osobowych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.
- 2.3. Zbiór danych osobowych** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
- 2.4. RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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) z dnia 27 kwietnia 2016 r. (Dz.Urz.U.E.L Nr 119, str. 1).

- 2.5. Rejestr** – rejestr czynności przetwarzania danych, prowadzony zgodnie z art. 30 ust. 1 RODO oraz rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, prowadzony zgodnie z art. 30 ust. 2 RODO. Obydwa rejestry znajdują się w jednym dokumencie.
- 2.6. PSS – PODWAWELSKA SPÓŁDZIELNIA SPOŻYWCÓW z siedzibą w Krakowie** (adres al. Daszyńskiego 3, 31-537 Kraków), wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod nr 0000065020, NIP: 6750003448, będąca administratorem danych, tj. podmiotem ustalającym cele i sposoby przetwarzania danych osobowych.

3. Zasady dotyczące przetwarzania danych osobowych (art. 5 RODO)

Dane osobowe w PSS są:

3.1. Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”).

- 3.1.1. Zgodność przetwarzania danych osobowych z prawem** zapewniono poprzez zasięgnięcie w tym zakresie porady kancelarii prawnej. Istotne zagadnienia związane z przetwarzaniem danych osobowych są konsultowane z kancelarią prawną na bieżąco. PSS powierzy wewnętrznemu działowi administracyjnemu okresowe prowadzenie szkoleń dla zespołu PSS z zakresu ochrony danych osobowych.

PSS dąży do zapewnienia ciągłej zgodności z prawem przetwarzania danych osobowych. Obejmuje to okresowe (dokonywane nie rzadziej niż raz na 12 miesięcy) oceny i aktualizacje niniejszej Polityki ochrony danych osobowych. Jednym z kryteriów oceny powinna być zgodność z ewentualnymi kodeksami postępowania przyjętymi dla branży handlowo-usługowej, zgodnie z art. 40 i nast. RODO.

W razie potrzeby, niezwłocznej aktualizacji podlegają również informacje podawane osobom, których dane dotyczą, zgodnie z art. 13 i 14 RODO. W zakresie w jakim PSS bazuje na zgodzie, jako podstawie prawnej przetwarzania danych osobowych – zgody podlegają odnowieniu po każdej zmianie informacji udzielanych zgodnie z art. 4 ust. 11 w związku z motywem 42 RODO.

- 3.1.2. Podstawy prawne przetwarzania danych** osobowych wymieniono w Rejestrze.

PSS opiera się na przesłance legalizacyjnej z art. **6 ust. 1 lit b) RODO** (***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***) co do następujących operacji przetwarzania danych osobowych **klientów (tj. podmiotów dokonujących zakupów w sklepach prowadzonych przez PSS, przy czym**

PSS zaznacza, że relatywnie rzadko przetwarza jakiegokolwiek dane osobowe klientów):

- przygotowywanie ofert dla klienta,
- negocjowanie i zawieranie umów z klientem,
- kontaktowanie się z klientem za pośrednictwem email oraz archiwizacja korespondencji email,
- kontaktowanie się z klientem za pośrednictwem korespondencji tradycyjnej i archiwizacja tej korespondencji,
- telefoniczne kontaktowanie się z klientem.

PSS opiera się na przesłance wykonania umowy również co do następujących operacji przetwarzania danych osobowych **dostawców (tj. podmiotów od których PSS zakupuje towary lub usługi):**

- wysyłanie zapytań ofertowych,
- negocjowanie i zawieranie umów z dostawcą,
- kontaktowanie się z dostawcą za pośrednictwem email oraz archiwizacja korespondencji email,
- kontaktowanie się z dostawcą za pośrednictwem korespondencji tradycyjnej i archiwizacja tej korespondencji,
- telefoniczne kontaktowanie się z dostawcą.

PSS opiera się na przesłance wykonania umowy również co do następujących operacji przetwarzania danych osobowych **najemców (tj. podmiotów którym PSS wynajmuje lokale na prowadzenie działalności gospodarczej w budynku będącym własnością PSS):**

- przygotowywanie ofert dla najemcy,
- negocjowanie i zawieranie umów z najemcą,
- kontaktowanie się z najemcą za pośrednictwem email oraz archiwizacja korespondencji email,
- kontaktowanie się z najemcą za pośrednictwem korespondencji tradycyjnej i archiwizacja tej korespondencji,
- telefoniczne kontaktowanie się z najemcą.

PSS opiera się na przesłance legalizacyjnej z art. 6 ust. 1 lit c) RODO (**przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze**) co do następujących operacji przetwarzania danych osobowych **pracowników PSS i członków ich rodzin:**

- prowadzenie i archiwizacja dokumentacji pracowniczej zgodnie z art. 125a ust. 4. w zw. z art. 4. pkt 13 ustawy o emeryturach i rentach z FUS,
- zgłoszenie pracowników i członków ich rodzin do ZUS, aktualizacja zgłoszeń i przekazywanie danych o zwolnieniach, zgodnie z wymogami przepisów prawa, a przede wszystkim prawa ubezpieczeń społecznych;
- prowadzenie rozliczeń z pracownikami, wypłata wynagrodzeń naliczanie obciążeń oraz naliczanie składek do ZUS (odprowadzanie za pracowników zaliczek na podatek dochodowy oraz sporządzanie PIT, prowadzenie rachunkowości oraz realizacja obowiązków podatkowych przez PSS),

zgodnie z wymogami przepisów prawa, a przede wszystkim prawa pracy i prawa ubezpieczeń społecznych;

- prowadzenie ewidencji czasu pracy (zgodnie z Kodeksem pracy);
- przeszkolenie z zakresu BHP;
- prowadzenie badań zdolności do pracy (wstępnych i okresowych);
- prowadzenie badań zdrowotnych dla pracowników w zawiązku z koniecznością uzyskania przez niego aktualnego orzeczenia lekarskiego do celów sanitarno-epidemiologicznych.

Dla wykonania obowiązków wynikających z przepisów prawa przetwarzane są również dane osobowe **klientów, dostawców i najemców PSS**, co obejmuje następujące operacje przetwarzania danych:

- prowadzenie rachunkowości oraz archiwizacja dokumentów zgodnie z wymogami przepisów podatkowych.

Dla wykonania obowiązków wynikających z przepisów prawa przetwarzane są również dane osobowe **członków PSS (tj. członków Spółdzielni, zgodnie z ustawą prawo spółdzielcze, oraz osób ubiegających się o takie członkostwo)**, co obejmuje następujące operacje przetwarzania danych:

- zbieranie danych osobowych obejmujących imię, nazwisko, datę urodzenia, adres zamieszkania, zawód (w formie pisemnej deklaracji przystąpienia do spółdzielni) oraz archiwizację tych danych,
- informowanie członków o dacie i miejscu posiedzenia organu PSS, w którym członek ma prawo uczestniczyć,
- prowadzenie rachunkowości oraz archiwizacja dokumentów zgodnie z wymogami prawa podatkowego, w tym wypełnianie i przesyłanie członkom deklaracji podatkowych w razie skorzystania przez członka z nieodpłatnych świadczeń zapewnianych przez PSS (np. darmowe bilety do teatru).

PSS opiera się na przesłance legalizacyjnej z art. **6 ust. 1 lit f) RODO (przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora)** co do następujących operacji przetwarzania danych osobowych **pracowników**:

- utworzenie służbowych kont pracownika w aplikacjach służących do wykonywania obowiązków pracowniczych (w tym w szczególności w aplikacji obsługującej pocztę elektroniczną, aplikacji PC Market, aplikacji Płatnik i aplikacji Optima);
- udostępnienie danych osobowych pracownika klientom, dostawcom, najemcom i członkom, w zakresie w jakim to jest konieczne do wykonywania przez pracownika obowiązków,
- sprawowanie nadzoru nad pracownikiem (w tym w przypadkach wykonywania pracy zdalnej), co może obejmować wgląd do służbowej poczty elektronicznej pracownika (przy czym nie jest to monitoring systematyczny, a jedynie incydentalny, w razie odejścia pracownika lub kontraktora z PSS lub konieczności zastąpienia go na czas nieobecności inną osobą);

- utrwalanie, przechowywanie i w niezbędnym zakresie wgląd do zapisów obrazu z monitoringu wizyjnego, którym objęte jest częściowo miejsce pracy.

PSS, opierając przetwarzanie danych osobowych pracowników na podstawie prawnej określonej w art. 6 ust. 1 lit. f) RODO wzięła pod uwagę interesy oraz podstawowe prawa i wolności osób, których dane dotyczą. W ocenie PSS, te interesy, prawa i wolności nie przeważają nad prawnie uzasadnionymi interesami realizowanymi przez PSS, tj. prawem do sprawowania nadzoru nad pracownikiem i zapewnienia ciągłości działania przedsiębiorstwa w wypadku odejścia lub nieobecności dalej osoby (co do wglądu do służbowej poczty elektronicznej) oraz chęcią zagwarantowania bezpieczeństwa osób i ochrony mienia (co do monitoringu wizyjnego).

W ocenie PSS, oparcie przetwarzania danych osobowych pracowników na podstawie przewidzianej w art. 6 ust. 1 lit. f) RODO znajduje podstawę również w motywie 47 RODO. Mianowicie, w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z PSS, nadrzędne nie są interesy lub podstawowe prawa i wolności tych osób. Zachodzi bowiem istotny i odpowiedni rodzaj powiązania między osobami, których dane dotyczą a PSS.

Jednocześnie operacje przetwarzania danych dokonywane w oparciu o tę przesłankę zostały przez PSS tak dobrane, aby nie niosły ze sobą ryzyka naruszenia praw i wolności pracowników (np. poprzez ujawnienie ich danych podmiotom trzecim lub też tworzenie profili czy ocen).

Zmniejszeniu ryzyka naruszenia praw i wolności pracowników służy też przyjęta przez PSS polityka retencji danych osobowych.

Należy wreszcie wskazać, że PSS nie mogła oprzeć żadnej z wymienionych operacji przetwarzania na zgodzie pracowników jako przesłance legalizacyjnej, ponieważ zgoda taka nie byłaby udzielona w sposób dobrowolny, zważywszy na wyraźne zastrzeżenia czynione przez Grupę Roboczą art. 29 w Guidelines on Consent under Regulation 2016/679, a także samą definicję zgody zawartą w art. 4 ust. 11 RODO („*dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych*”). Pomiędzy pracownikiem i PSS zachodzi bowiem wyraźny „brak równowagi stron” w rozumieniu motywu 43 RODO. Co nawet ważniejsze, brak udzielenia zgody skutkowałby koniecznością rozwiązania umowy z pracownikiem. Ewentualna zgoda byłaby więc na gruncie RODO nieskuteczna.

PSS opiera się na przesłance legalizacyjnej z art. 6 ust. 1 lit. f) RODO również co do następujących operacji przetwarzania danych osobowych **kandydatów do pracy w PSS** (wszystkie we wspólnym celu – tj. w celu prowadzenia ciągłej rekrutacji pracowników):

- zbieranie danych osobowych zawartych w CV oraz innych dokumentach dostarczonych przez kandydata do PSS,

- weryfikacja przydatności kandydata na określone stanowiska pracy poprzez analizę zebranych danych osobowych, a także (na dalszym etapie rekrutacji) poprzez prowadzenie rozmów kwalifikacyjnych,
- kontaktowanie się z kandydatem przez email oraz telefonicznie,
- przechowywanie danych osobowych kandydata przez okres 12 miesięcy.

PSS, opierając przetwarzanie danych osobowych kandydatów na podstawie prawnej określonej w art. 6 ust. 1 lit. f) RODO wzięła pod uwagę interesy oraz podstawowe prawa i wolności osób, których dane dotyczą. W ocenie PSS, te interesy, prawa i wolności nie przeważają nad prawnie uzasadnionymi interesami realizowanymi przez PSS.

Jednocześnie operacje przetwarzania danych dokonywane w oparciu o tę przesłankę zostały przez PSS tak dobrane, aby nie niosły ze sobą ryzyka naruszenia praw i wolności kandydatów (np. poprzez nadmierny zakres przetwarzanych danych).

Zmniejszeniu ryzyka naruszenia praw i wolności kandydatów służy też przyjęta przez PSS polityka retencji danych osobowych.

PSS opiera się na przesłance legalizacyjnej z art. 6 ust. 1 lit. f) RODO również co do następujących operacji przetwarzania danych osobowych **użytkowników strony internetowej <http://www.podwawelska.pl/>**

- automatyczny odczyt unikalnego oznaczenia identyfikującego zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzysta użytkownik (adres IP) a także parametrów technicznych urządzenia i oprogramowania wykorzystywanego przez użytkownika (jak rodzaj przeglądarki, czy rozdzielczość monitora) oraz wykorzystanie tych danych w celach statystycznych i dla poprawy funkcjonowania strony.

PSS, opierając przetwarzanie danych osobowych użytkowników strony na podstawie prawnej określonej w art. 6 ust. 1 lit. f) RODO wzięła pod uwagę interesy oraz podstawowe prawa i wolności osób, których dane dotyczą. W ocenie PSS te interesy, prawa i wolności nie przeważają nad prawnie uzasadnionymi interesami realizowanymi przez PSS, tj. prawem do prowadzenia badań statystycznych.

W ocenie PSS, oparcie przetwarzania danych osobowych użytkowników na podstawie przewidzianej w art. 6 ust. 1 lit. f) RODO znajduje podstawę również w motywie 47 RODO. Mianowicie, w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z PSS, nadrzędne nie są interesy lub podstawowe prawa i wolności tych osób. Zachodzi bowiem istotny i odpowiedni rodzaj powiązania między osobami, których dane dotyczą a PSS.

Jednocześnie operacje przetwarzania danych dokonywane w oparciu o tę przesłankę zostały przez PSS tak dobrane, aby nie niosły ze sobą ryzyka naruszenia praw i wolności użytkowników (np. poprzez nadmierny zakres zbieranych danych, ich ujawnianie podmiotom trzecim, czy poddawanie profilowaniu).

Zmniejszeniu ryzyka naruszenia praw i wolności użytkowników strony służy też przyjęta przez PSS polityka retencji danych osobowych.

PSS opiera się na przesłance legalizacyjnej z art. 6 ust. 1 lit f) RODO również co do następujących operacji przetwarzania danych osobowych **osób odwiedzających sklepy prowadzone przez PSS:**

- utrwalanie, przechowywanie i w niezbędnym zakresie wgląd do zapisów obrazu z monitoringu wizyjnego, którym objęte są sklepy prowadzone przez PSS.

PSS, opierając przetwarzanie danych osobowych odwiedzających na podstawie prawnej określonej w art. 6 ust. 1 lit. f) RODO wzięła pod uwagę interesy oraz podstawowe prawa i wolności osób, których dane dotyczą. W ocenie PSS te interesy, prawa i wolności nie przeważają nad prawnie uzasadnionymi interesami realizowanymi przez PSS, tj. chęcią zagwarantowania bezpieczeństwa osób i ochrony mienia.

W ocenie PSS, oparcie przetwarzania danych osobowych odwiedzających na podstawie przewidzianej w art. 6 ust. 1 lit. f) RODO znajduje podstawę również w motywie 47 RODO. Mianowicie, w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z PSS, nadrzędne nie są interesy lub podstawowe prawa i wolności tych osób. Zachodzi bowiem istotny i odpowiedni rodzaj powiązania między osobami, których dane dotyczą a PSS.

Jednocześnie operacje przetwarzania danych dokonywane w oparciu o tę przesłankę zostały przez PSS tak dobrane, aby nie niosły ze sobą ryzyka naruszenia praw i wolności odwiedzających (np. poprzez nadmierny zakres zbieranych danych, czy jakiegokolwiek opracowywanie).

Zmniejszeniu ryzyka naruszenia praw i wolności odwiedzających służy też przyjęta przez PSS polityka retencji danych osobowych.

PSS opiera się na przesłance legalizacyjnej z art. 6 ust. 1 lit f) RODO również co do następujących operacji przetwarzania danych osobowych **klientów, dostawców, najemców, pracowników i członków (a także byłych klientów, dostawców, najemców, pracowników i członków):**

- dochodzenie roszczeń w wypadku naruszenia umowy z PSS (lub statutu), lub też w razie wyrządzenia szkody PSS w inny sposób.

PSS, opierając przetwarzanie danych osobowych tych kategorii osób na podstawie prawnej określonej w art. 6 ust. 1 lit. f) RODO wzięła pod uwagę interesy oraz podstawowe prawa i wolności osób, których dane dotyczą. W ocenie PSS te interesy, prawa i wolności nie przeważają nad prawnie uzasadnionymi interesami realizowanymi przez PSS, tj. chęcią ochrony swych praw i dochodzenia naprawienia szkody.

W ocenie PSS, oparcie przetwarzania danych osobowych odwiedzających na podstawie przewidzianej w art. 6 ust. 1 lit. f) RODO znajduje podstawę również w motywie 47 RODO. Mianowicie, w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z PSS, nadrzędne nie są interesy lub podstawowe prawa i wolności tych osób. Zachodzi bowiem

istotny i odpowiedni rodzaj powiązania między osobami, których dane dotyczą a PSS.

Jednocześnie operacje przetwarzania danych dokonywane w oparciu o tę przesłankę zostały przez PSS tak dobrane, aby nie niosły ze sobą ryzyka naruszenia praw i wolności odwiedzających.

Zmniejszeniu ryzyka naruszenia praw i wolności odwiedzających służy też przyjęta przez PSS polityka retencji danych osobowych.

PSS opiera się na przesłance legalizacyjnej z art. **28 RODO (jest podmiotem przetwarzającym dane osobowe dla podmiotu trzeciego, będącego administratorem danych)** co do następujących operacji przetwarzania danych osobowych **pracowników i ich osób bliskich**:

- zbieranie i przekazywanie **Towarzystwo Ubezpieczeń na Życie „Warta” S.A. z siedzibą w Warszawie ul.Chmielna 85/87** (w związku z zawartym w dniu 25.05.2018 Aneksem) danych osobowych pracowników i ich osób bliskich koniecznych do wypełnienia formularzy aplikacyjnych przygotowanych przez towarzystwo ubezpieczeniowe, a także archiwizację tych danych (w formie kopii zapasowych) i ich aktualizację oraz spełnianie w imieniu administratora obowiązku informacyjnego;
- zbieranie i przekazywanie **Benefit Systems Spółka Akcyjna z siedzibą w Warszawie** (w związku z zawartym w dniu 15 marca 2018 Aneksem nr 3 do umowy o świadczenie usług) danych osobowych pracowników i ich osób bliskich koniecznych do wypełnienia formularzy aplikacyjnych przygotowanych przez Benefit Systems Spółka Akcyjna z siedzibą w Warszawie, a także archiwizację tych danych (w formie kopii zapasowych) i ich aktualizację;
- przetwarzanie danych osobowych osób skierowanych do świadczenia usług w PSS przez **p. Vadyma Zanfirowa prowadzącego działalność gospodarczą pod nazwą „Firma Anna”**, zgodnie z umową świadczenia usług zawartą w dniu 8 grudnia 2015 roku oraz umową powierzenia danych do przetwarzania zawartą w dniu 01.06.2018.

3.1.3. **Rzetelność i przejrzystość przetwarzania danych osobowych** zagwarantowano poprzez wdrożenie Rejestru oraz zapewniając osobom, których dane dotyczą informacje wymagane na podstawie art. 13, 14 i 21. ust. 4. RODO.

Informacje udzielane na podstawie art. 13 i 14 RODO, a także art. 4 ust 11 RODO zostały przygotowane i są aktualizowane w oparciu o wytyczne Grupy Roboczej art. 29 zawarte w Guidelines on transparency under Regulation 2016/679.

3.2. Zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”).

3.2.1. Cele przetwarzania danych osobowych przez PSS opisano w Rejestrze.

3.2.2. W przypadku danych osobowych pozyskiwanych przez PSS nie od osób, których one dotyczą (dane osób bliskich pracowników PSS) – w myśl art. 6 ust. 4 RODO, ustalono, że przetwarzanie danych osobowych odbiorców

odbywa się w tym samym celu, dla którego zostały pierwotnie zebrane przez pracownika ujawniającego je PSS. Nie ma więc potrzeby dokonywania oceny zgodnie z art. 6 ust. 4 RODO.

3.2.3. Informacje udzielane zgodnie z art. 14 RODO obejmują m.in. treść ust. 3.2.2. powyżej.

3.3. Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”).

3.3.1. W zakresie w jakim dane osobowe przetwarzane są dla innych celów niż realizacja obowiązków nałożonych przez przepisy prawa, PSS regularnie (nie rzadziej niż raz na 12 miesięcy) dokonuje przeglądu tych danych i – w razie takiej możliwości – ich minimalizacji (przez zaprzestanie zbierania, usunięcie lub anonimizację).

3.3.2. PSS nie dokonuje żadnych operacji na danych osobowych i nie przetwarza żadnych danych osobowych, które nie są konieczne dla założonych celów i w sposób z gruntu nieuczciwy, nawet na podstawie zgody osoby, której dane dotyczą (w myśl wytycznych Grupy Roboczej art. 29 zawartych w pkt 1 Guidelines on Consent under Regulation 2016/679 oraz w Opinion 15/2011 on the definition of consent).

3.4. Prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”).

3.4.1. PSS wdraża procedury mające na celu okresową (nie rzadziej niż raz na 12 miesięcy) aktualizację danych osobowych.

3.5. 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 („ograniczenie przechowywania”).

3.5.1. Okresy przechowywania danych osobowych opisano w Rejestrze.

3.5.2. Retencja znacznej części danych osobowych klientów i dostawców, najemców, członków a także pracowników PSS wynika z przepisów prawa. Pozostałe dane dotyczące tych osób przetwarzane są przez okres (i w zakresie) niezbędnym dla realizacji umowy (statutu), w tym wynikających z niej roszczeń, pozostających w mocy również po wygaśnięciu samej umowy (np. o zapłatę wynagrodzenia, roszczeń regresowych, odszkodowawczych, kar umownych, związanych z zawartą umową o poufności), do upływu przedawnienia tych roszczeń.

3.5.3. Retencja danych eksploatacyjnych użytkowników strony internetowej (IP) określona jest szczegółowo w Polityce Cookies dostępnej tutaj: www.podwawelska.pl

3.5.4. Retencja zapisów obrazu z monitoringu wizyjnego wynosi nie więcej niż 30 dni.

3.6. 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 („integralność i poufność”).

- 3.6.1. Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i możliwości rozliczenia przetwarzanych danych zawarto w Rejestrze.

4. Realizacja uprawnień osób, których dane dotyczą

PSS wprowadza następujące procedury pozwalające na zgodną z prawem i przejrzystą realizację uprawnień osób, których dane dotyczą:

4.1. Reagowanie na żądanie udzielenia dostępu do danych osobowych, zgłoszone na podstawie art. 15 RODO.

- 4.1.1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od PSS, jako administratora danych osobowych, potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz do informacji przewidzianych przepisami prawa.
- 4.1.2. PSS dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, PSS może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną (np. za pośrednictwem poczty elektronicznej). Przy czym prawo do uzyskania takiej kopii nie może niekorzystnie wpływać na prawa i wolności innych osób.
- 4.1.3. Osoba uprawniona może zgłosić, żądanie o którym mowa w pkt. 4.1.1. powyżej w dowolnej formie, przy czym szczegółowe informacje co do możliwych form zgłoszenia takiego żądania znajdują się we właściwej polityce prywatności.
- 4.1.4. PSS, po weryfikacji, czy zapytanie pochodzi od uprawnionej osoby, tak by wykluczyć uzyskanie informacji przez osobę nieuprawnioną, udzieli takiej informacji w formie oczekiwanej przez osobę uprawnioną, w szczególności w takiej samej w jakiej zgłoszono żądanie.

4.2. Reagowanie na żądanie sprostowania danych osobowych, zgłoszone na podstawie art. 16 RODO.

- 4.2.1. Osoba, której dane dotyczą, ma prawo żądania od PSS, jako administratora danych osobowych, niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
- 4.2.2. Podobnie, z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania od PSS, jako administratora danych osobowych, uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
- 4.2.3. Osoba uprawniona może zgłosić, żądanie o którym mowa w pkt. 4.2.1. powyżej w dowolnej formie, przy czym szczegółowe informacje co do możliwych form zgłoszenia takiego żądania znajdują się we właściwej polityce prywatności.

4.2.4. PSS, po weryfikacji, czy żądanie pochodzi od uprawnionej osoby, tak by wykluczyć dokonanie zmian na żądanie osoby nieuprawnionej, dokona takiego sprostowania we wszystkich systemach.

4.3. Reagowanie na żądanie zaprzestania przetwarzania danych (w tym skorzystania z prawa do bycia zapomnianym), zgłoszone na podstawie art. 17 RODO.

4.3.1. Osoba, której dane dotyczą, ma prawo żądania od PSS niezwłocznego usunięcia dotyczących jej danych osobowych, a PSS bez zbędnej zwłoki usunie jej dane osobowe, jeżeli istnieją ku temu przyczyny przewidziane w przepisach prawa oraz gdy nie ma podstaw prawnych do dalszego ich przetwarzania.

4.3.2. Jeżeli PSS udostępnia dane osobowe innym podmiotom, a ma obowiązek usunąć te dane osobowe, to podejmie wszelkie dostępne działania, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje. Biorąc pod uwagę fakt, że PSS zna wszystkie podmioty, którym dane osobowe udostępnia, poinformowanie tych podmiotów nastąpi niezwłocznie.

4.3.3. Osoba uprawniona może zgłosić, żądanie o którym mowa w pkt. 4.3.1. powyżej w dowolnej formie, przy czym szczegółowe informacje co do możliwych form zgłoszenia takiego żądania znajdują się we właściwej polityce prywatności.

4.3.4. PSS, po weryfikacji, czy żądanie pochodzi od uprawnionej osoby, tak by wykluczyć naruszenie praw lub wolności innych osób, natychmiast zaprzestanie przetwarzania danych osobowych żądającego oraz usunie wszystkie jego dane osobowe ze wszystkich systemów oraz wykona działania wskazane w pkt 4.3. powyżej, zgodnie z przepisami prawa.

4.4. Reagowanie na żądanie ograniczenia przetwarzania danych, zgłoszone na podstawie art. 18 RODO.

4.4.1. Osoba, której dane dotyczą, ma prawo żądania od PSS ograniczenia przetwarzania jej danych osobowych w przypadkach przewidzianych w przepisach prawa.

4.4.2. Jeżeli przetwarzanie zostało ograniczone zgodnie z przepisami prawa, takie dane osobowe PSS może przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

4.4.3. Przed uchycieniem ograniczenia przetwarzania PSS informuje o tym osobę, która żądała ograniczenia.

4.4.4. PSS niezwłocznie dokona ograniczenia przetwarzania danych osobowych osoby, która zgłosiła żądanie o którym mowa w pkt. 4.4.1. powyżej, przy czym uprzednio zweryfikuje, czy żądanie pochodzi od uprawnionej osoby, tak by wykluczyć naruszenie praw lub wolności innych osób.

4.4.5. Osoba uprawniona może zgłosić, żądanie o którym mowa w pkt. 4.4.1. powyżej w dowolnej formie, przy czym szczegółowe informacje co do możliwych form zgłoszenia takiego żądania znajdują się we właściwej polityce prywatności.

4.5. Reagowanie na żądanie przeniesienia danych, zgłoszone na podstawie art. 20 RODO.

4.5.1. PSS na żądanie osoby, której dane dotyczą, dostarczy jej w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła PSS.

4.5.2. PSS będzie dostarczać dane w formie plików XML, JSON lub CSV i nie będzie czynić żadnych przeszkód by dane, dostarczone zgodnie z pkt 4.5.1. powyżej, zostały przekazane innemu administratorowi przez uprawnioną osobę.

4.5.3. Ponadto, PSS wykonując prawo do przenoszenia danych, o którym mowa w pkt. 4.5.1. powyżej, na żądanie osoby, której dane dotyczą prześle te dane bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

4.5.4. Osoba uprawniona może zgłosić, żądanie o którym mowa w pkt. 4.5.1. powyżej w dowolnej formie, przy czym szczegółowe informacje co do możliwych form zgłoszenia takiego żądania znajdują się we właściwej polityce prywatności.

4.5.5. PSS, po weryfikacji, czy żądanie pochodzi od uprawnionej osoby, tak by wykluczyć naruszenie praw lub wolności innych osób, niezwłocznie dostarczy żądane dane, zgodnie z pkt. 4.5.1.-4.5.3. powyżej, w sposób indywidualnie ustalony z osobą uprawnioną.

4.6. Reagowanie na sprzeciw co do przetwarzania danych, zgłoszony na podstawie art. 21 RODO.

4.6.1. Jeśli osoba uprawniona wniesie sprzeciw wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, w tym profilowania na podstawie tych przepisów, PSS zaprzestanie przetwarzania tych danych, chyba że będą istniały ważne, prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

4.6.2. PSS zaprzestanie również przetwarzania (w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim) danych osobowych, które były przetwarzane na potrzeby marketingu bezpośredniego (w tym profilowania), jeśli osoba, której dane dotyczą, wniesie sprzeciw wobec ich przetwarzania.

4.6.3. PSS wyraźnie, jasno i odrębnie od wszelkich innych informacji, informuje, najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, o prawie do wniesienia sprzeciwu, o którym mowa w pkt. 4.6.2. powyżej.

4.6.4. Osoba uprawniona może zgłosić, żądanie o którym mowa w pkt. 4.6.1. lub 4.6.2. powyżej w dowolnej formie, przy czym szczegółowe informacje co do możliwych form zgłoszenia takiego żądania znajdują się we właściwej polityce prywatności.

- 4.7. PSS informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Przy czym ze względu na fakt, że PSS zna odbiorców danych osobowych powyższy obowiązek informacyjny nie powinien nastęrczać problemów. Ponadto, PSS informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
- 4.8. W PSS jest zatrudniona osoba, której zadaniem jest dbanie o zachowanie zasad i wymogów ochrony danych osobowym, w tym wypełnianie obowiązków o których mowa w pkt. 4.1.-4.6. powyżej. Osoba ta posiada odpowiednią wiedzę z zakresu ochrony danych osobowych i jest odpowiednio przeszkolona w tym zakresie.
- 4.9. Osoba, o której mowa w pkt. 4.8. powyżej, na bieżąco dba by żądania osób uprawnionych były weryfikowane i wykonywane zgodnie z przepisami prawa oraz wewnętrznymi politykami.
- 4.10. Oprogramowanie służące do przetwarzania danych osobowych w PSS posiada narzędzia umożliwiające spełnienie wymogów RODO, w szczególności w zakresie wyszukiwania danych osobowych, ich zmiany, generowania informacji dla uprawnionych i skutecznego usunięcia.
- 4.11. Wszystkie działania, o których mowa pkt. 4.1.-4.6. powyżej, będą stosowane do wszystkich nośników danych – zarówno elektronicznych (w tym backupów danych), jak i w formie wydruków, przetwarzanych przez PSS oraz podmioty przetwarzające dane dla PSS (w trybie art. 28 RODO). Odpowiednie umowy z podmiotami przetwarzającymi dane osobowe dla PSS w trybie art. 28 RODO uprawniają PSS do żądania podjęcia analogicznych działań również przez te podmioty.
- 4.12. Do danych osobowych, co do których PSS jest jedynie podmiotem przetwarzającym (w trybie art. 28 RODO), niniejszy rozdział nie stosuje się. W razie zgłoszenia któregośkolwiek z opisanych żądań PSS dokonuje niezwłocznego zawiadomienia administratora o zgłoszeniu, i postępuje zgodnie z procedurą przewidzianą w odpowiedniej umowie zawartej z administratorem.

5. Zgłoszenie naruszenia ochrony danych osobowych (art. 33 i 34 RODO)

- 5.1. Stosując niniejszy rozdział Polityki ochrony danych osobowych, powinno się zawsze na pierwszym miejscu stawiać ochronę osób, których dane przetwarzane są przez PSS. Na potrzeby niniejszego rozdziału przez „pracownika” rozumie się osobę zatrudnioną w PSS, niezależnie od podstawy prawnej zatrudnienia.
- 5.2. Zgodnie z wytycznymi Grupy Roboczej art. 29, zawartymi we wstępie do Guidelines on Personal data breach notification under Regulation 2016/679, rozdział został podzielony na podrozdziały omawiające wykrycie, ograniczenie, ocenę ryzyka naruszenia praw i wolności osób, podejmowanie decyzji nt. zgłoszenia naruszenia organowi nadzorczemu oraz zawiadomienia osób, których dane dotyczą, a także procedurę dokonywania zgłoszenia i zawiadomienia.
- 5.3. **Wykrycie naruszenia.**
 - 5.3.1. W rozdziale I lit. B pkt 2 Guidelines on personal data breach notification under Regulation 2016/679 zawarto ogólną klasyfikację rodzajów naruszeń ochrony danych. I tak, Grupa Robocza art. 29 wyróżnia:

- naruszenie poufności (oznaczające nieuprawnione lub przypadkowe ujawnienie danych osobowych lub umożliwienie dostępu do nich osobie trzeciej)
- naruszenie integralności (oznaczające nieuprawnioną lub przypadkową zmianę treści danych osobowych)
- utratę dostępu (oznaczającą nieuprawnione lub przypadkowe zniszczenie danych osobowych lub utratę dostępu do nich).

5.3.2. PSS dokłada starań, aby wykrycie naruszenia danych osobowych było możliwe w jak najkrótszym czasie od chwili naruszenia. I tak:

- naruszenia danych osobowych polegające na włamaniu do pomieszczeń, w których przetwarzane są dane osobowe lub na zniszczeniu tych pomieszczeń (np. w wyniku pożaru) są natychmiastowo raportowane PSS przez pracowników, którzy zostali przeszkoleni w tym zakresie;
- naruszenia danych osobowych polegające na utracie (zniszczeniu, kradzieży) mobilnych urządzeń elektronicznych, służących do przetwarzania danych osobowych (laptopy, telefony), a także polegające na błędach lub zaniedbaniach pracowników PSS (np. zgubienie nośnika USB zawierającego dane osobowe, albo omyłkowe wysłanie wiadomości zawierającej dane osobowe na niewłaściwy adres poczty elektronicznej) są zgłaszane natychmiastowo przez samych pracowników (pracownicy zostali w tym zakresie przeszkoleni);
- naruszenia danych osobowych polegające na awarii oprogramowania służącego do przetwarzania danych osobowych lub uzyskaniu do niego dostępu przez osoby nieuprawnione (atak hackerski) powinny być zgłaszane PSS niezwłocznie przez podmioty udostępniające tę infrastrukturę PSS w modelu IaaS¹ (PSS podejmuje stosowne kroki w celu zagwarantowania takiego obowiązku informacyjnego w umowie łączącej ją z dostawcami infrastruktury) zaś w razie awarii lub ataku hackerskiego w ramach środowiska informatycznego PSS ich niezwłocznie wykrycie jest gwarantowane przez odpowiednie oprogramowanie monitorujące,
- naruszenia danych osobowych przez podmioty przetwarzające dane osobowe dla PSS w rozumieniu art. 28 RODO są zgłaszane natychmiastowo przez te podmioty zarządowi PSS lub upoważnionemu pracownikowi PSS (podmioty te zostały zobowiązane do takiego działania w stosownych umowach).

5.4. Ograniczenie zasięgu naruszenia.

5.4.1. Każdy pracownik PSS, który wykryje naruszenie ochrony danych osobowych informuje przełożonego działu, w którego ramach doszło do naruszenia. Gdy nie jest to możliwe do natychmiastowego wykonania, pracownik informuje swojego bezpośredniego przełożonego.

¹ Szczecinie).

Według stanu na kwiecień 2018 roku dotyczy to hostingu poczty elektronicznej (home.pl S.A. z siedzibą w

- 5.4.2. W razie gdy naruszenie danych zostaje wykryte przez pracownika poza godzinami pracy (w tym np. w trakcie urlopu), obowiązek natychmiastowego poinformowania przełożonego obowiązuje bez zmian.
- 5.4.3. Przełożony informuje o naruszeniu zarząd PSS.
- 5.4.4. Zarząd niezwłocznie, jednak nie później niż w ciągu 24 godzin, zwołuje Zespół do Spraw Naruszeń Ochrony Danych. W skład zespołu wchodzi każdorazowo przynajmniej jeden członek Zarządu, Pani Adrianna Marcisz, przełożony działu, w którym doszło do naruszenia oraz – jeśli to możliwe – przedstawiciel kancelarii prawnej obsługującej PSS.
- 5.4.5. Przełożony działu, w którym doszło do naruszenia identyfikuje zdarzenie, jako należące do jednej z trzech kategorii:
- rzeczywiste lub prawdopodobne naruszenie ochrony danych osobowych,
 - incydent bezpieczeństwa systemu informatycznego, niebędący naruszeniem ochrony danych osobowych,
 - inny rodzaj incydentu bezpieczeństwa, narażającego dane osobowe na ryzyko naruszenia, ale niebędący naruszeniem ochrony danych osobowych.
- 5.4.6. Przełożony działu, w którym doszło do naruszenia ochrony danych osobowych zbiera wszelkie informacje dotyczące tego zdarzenia i dostarcza je niezwłocznie Zespołowi do Spraw Naruszeń Ochrony Danych. W szczególności zebrane zostają następujące informacje:
- data i godzina wystąpienia zdarzenia i czasokres jego trwania,
 - data i godzina wykrycia zdarzenia,
 - osoba która wykryła zdarzenie,
 - opis zdarzenia,
 - przybliżona ilość osób, których zdarzenie może dotyczyć,
 - informacje o już podjętych krokach mających na celu zminimalizowanie lub ograniczenie oddziaływania zdarzenia na osoby, których dane dotyczą,
 - dane osób, które mają świadomość, że zdarzenie nastąpiło,
 - dane związanych ze zdarzeniem podwykonawców (podmiotów przetwarzających dane osobowe).
- 5.4.7. Przełożony działu, w którym doszło do naruszenia zapewni, aby jak najmniej osób w ramach PSS, a zwłaszcza poza PSS miało dostęp do informacji zebranych zgodnie z ust. 5.4.6. powyżej.
- 5.4.8. Ograniczenie zasięgu naruszenia ochrony danych osobowych obejmuje natychmiastowe zakończenie trwania zdarzenia oraz jak najszybszą minimalizację jego zakresu i wpływu na osoby, których dane dotyczą. W tym celu Zespół do Spraw Naruszeń Ochrony Danych podejmuje wiążące dla PSS decyzje w najszybszym możliwym czasie i przystępuje do ich realizacji. W szczególności Zespół do Spraw Naruszeń Ochrony Danych kontaktuje się z wybranymi osobami wewnątrz i spoza PSS.

5.5. Ocena ryzyka naruszenia praw i wolności osób, których dane dotyczą.

- 5.5.1. Zespół do Spraw Naruszeń Ochrony Danych wydaje opinię, czy zdarzenie stanowi naruszenie ochrony danych osobowych. W tym celu Zespół do Spraw Naruszeń Ochrony Danych posługuje się przede wszystkim wytycznymi Grupy Roboczej art. 29 zawartymi m.in. w Annex B do Guidelines on Personal data breach notification under Regulation 2016/679. Opinia ma formę pisemną.
- 5.5.2. W razie gdy zdarzenie zostaje zakwalifikowane jako naruszenie ochrony danych osobowych, Zespół do Spraw Naruszeń Ochrony Danych przeprowadza dochodzenie mające na celu ustalenie:
- czy naruszenie jest naruszeniem poufności, integralności czy utratą dostępu,
 - kategorie i ilość danych objętych naruszeniem,
 - wrażliwość danych,
 - jaki zakres informacji o osobach, których dane dotyczą, może być wyczytany z danych osobowych objętych naruszeniem,
 - liczbę osób dotkniętych skutkami naruszenia,
 - jaki rodzaj osób został dotknięty naruszeniem (np. klienci, kandydaci, pracownicy),
 - istniejące zabezpieczenia danych objętych naruszeniem (np. pseudonimizacja danych lub szyfrowanie nośnika),
 - czy dane mogą trafić w ręce osób trzecich i potencjalnie zostać wykorzystane w celu sprzecznym z prawem lub innym niewłaściwym celu.
- 5.5.3. Dochodzenie powinno być zakończone nie później niż w 36 godzin od chwili wykrycia naruszenia. Rezultaty dochodzenia są dokumentowane na piśmie.
- 5.5.4. Biorąc pod uwagę wyniki dochodzenia Zespół do Spraw Naruszeń Ochrony Danych wydaje w terminie 60 godzin od wykrycia naruszenia opinię, czy naruszenie ochrony danych osobowych wymaga zgłoszenia organowi nadzorczemu właściwemu zgodnie z art. 55 RODO lub zawiadomienia osób, których dane dotyczą. Opinia ma formę pisemną.
- 5.5.5. Przy wydawaniu opinii Zespół do Spraw Naruszeń Ochrony Danych kieruje się przede wszystkim tym, czy zaistniałe naruszenie może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfalszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne (zgodnie z motywem 85 RODO). Ponadto Zespół do Spraw Naruszeń Ochrony Danych kieruje się wytycznymi Grupy Roboczej art. 29 zawartymi w rozdziale II lit. A oraz D, jak też w rozdziale III lit. A oraz w rozdziale IV lit. A i B, a także w Annex B do Guidelines on Personal data breach notification under Regulation 2016/679.
- 5.5.6. Ilekroć Zespół do Spraw Naruszeń Ochrony Danych poweźmie wątpliwości, czy naruszenie ochrony danych wymaga zgłoszenia organowi nadzorczemu, albo gdy nie jest w tym zakresie jednomyślny – należy przyjąć, że zgłoszenie jest wymagane. W razie wątpliwości, czy naruszenie ochrony danych wymaga

zawiadomienia osób nim dotkniętych – PSS bezwzględnie zastosuje się w tym zakresie do rekomendacji organu nadzorczego.

- 5.5.7. W zakresie w jakim stwierdzone naruszenie dotyczy danych osobowych, co do których PSS jest jedynie podmiotem przetwarzającym (zgodnie z art. 28 RODO), pkt. 5.5.4.-5.5.6. a także pkt. 5.6. i 5.7. nie stosują się. W takim wypadku PSS dokonuje niezwłocznego zawiadomienia administratora o naruszeniu i postępuje zgodnie z procedurą przewidzianą w odpowiedniej umowie zawartej z administratorem.

5.6. Procedura dokonywania zgłoszenia i zawiadomienia.

- 5.6.1. W przypadku stwierdzenia zgodnie z niniejszym rozdziałem, że doszło do naruszenia ochrony danych osobowych podlegającego zgłoszeniu, PSS bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
- 5.6.2. Zgłoszenie naruszenia musi co najmniej:
- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
 - zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
 - opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
 - opisywać środki zastosowane lub proponowane przez PSS w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
- 5.6.3. W razie gdyby informacje wymagane zgodnie z ust. 5.6.2. tiret pierwsze powyżej nie były dostępne, PSS dokonuje zgłoszenia z podaniem danych przypuszczalnych lub przybliżonych. Przy dokonywaniu zgłoszenia należy koncentrować się na odwróceniu lub ograniczeniu skutków naruszenia, raczej niż na badaniu dokładnych liczb.
- 5.6.4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
- 5.6.5. **Wzór zgłoszenia stanowi Załącznik nr 1** do niniejszej Polityki ochrony danych osobowych.
- 5.6.6. W przypadku stwierdzenia zgodnie z niniejszym rozdziałem, że doszło do naruszenia ochrony danych osobowych wymagającego zawiadomienia osób, których dane dotyczą – PSS niezwłocznie zawiadamia takie osoby.
- 5.6.7. Zawiadomienie zawiera przynajmniej następujące informacje (art. 34 ust. 2 RODO oraz motyw 86 RODO):
- opis charakteru naruszenia ochrony danych osobowych,

- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opis możliwych konsekwencji naruszenia ochrony danych osobowych,
- opis środków zastosowanych lub proponowanych przez PSS w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków,
- zalecenia dla dotkniętych naruszeniem osób co do minimalizacji potencjalnych niekorzystnych skutków (np. dokonanie resetu haseł).

- 5.6.8. Zawiadomienie jest dokonywane jasnym i prostym językiem. Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania. Na przykład potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie (motyw 86 RODO).
- 5.6.9. PSS zawiadamia osoby dotknięte naruszeniem ochrony danych osobowych w sposób bezpośredni, chyba że wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skutecznym sposób.
- 5.6.10. W przypadku wyboru drogi elektronicznej (np. e-mail czy sms) w celu dokonania zawiadomienia, wiadomość taka będzie wysłana odrębnie (i będzie się wyraźnie różnić) od innych, regularnie wysyłanych, standardowych wiadomości (np. newslettera). Ma to zapewnić, że zawiadomienie nie pozostanie niezauważone przez odbiorcę. PSS w uzasadnionych wypadkach może zdecydować o zastosowaniu kilku sposobów zawiadomień jednocześnie (np. za pośrednictwem wiadomości e-mail i równolegle poczty tradycyjnej).
- 5.6.11. Z uwagi na fakt, że adresatami zawiadomienia mogą być osoby nieznające języka polskiego (zwłaszcza w wypadku gdy naruszenie dotyczy danych osobowych ze zbioru klientów sklepu internetowego), każde zawiadomienie powinno być dokonane – obok języka polskiego – co najmniej również w języku angielskim.
- 5.7.** PSS dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja obejmuje również zdarzenia, które nie zostały zakwalifikowane jako naruszenia ochrony danych osobowych po przeprowadzeniu procedury przewidzianej w niniejszym rozdziale, a także takie naruszenia ochrony danych osobowych, które nie zostały zgłoszone do organu nadzorczego. Dokumentacja obejmuje w szczególności rezultaty dochodzenia zgodnie z ust. 5.5.3. powyżej, jak też opinie wydane przez Zespół do Spraw Naruszeń Ochrony Danych zgodnie z ust. 5.5.1. i 5.5.4 powyżej. Dokumentacja pozwala organowi nadzorczemu na weryfikowanie przestrzegania art. 33 RODO przez PSS. **Wzór raportu z**

naruszenia ochrony danych osobowych stanowi Załącznik nr 2 do niniejszej Polityki ochrony danych osobowych, a **wzór ewidencji naruszeń ochrony danych osobowych stanowi Załącznik nr 3** do niniejszej Polityki ochrony danych osobowych.

6. Procedura zmiany i usuwania danych osobowych

Mając na uwadze, że dane osobowe należy usuwać w razie ustania ich przydatności do celu przetwarzania, a także m.in. w razie skutecznego zgłoszenia sprzeciwu lub żądania „bycia zapomnianym” przez osobę, której dane dotyczą, jak też w razie zgłoszenia do PSS takiego żądania przez administratora powierzającego PSS przetwarzanie danych w trybie art. 28 RODO – wprowadza się następującą procedurę gwarantującą pełne i bezpowrotne usunięcie danych:

- 6.1.** W PSS jest zatrudniona osoba, której zadaniem jest dbanie o zachowanie zasad i wymogów ochrony danych osobowych, w tym wypełnianie obowiązku zmiany bądź usunięcia danych osobowych. Osoba ta posiada odpowiednią wiedzę z zakresu ochrony danych osobowych i jest odpowiednio przeszkolona w tym zakresie.
- 6.2.** Osoba, o której mowa w pkt. 6.1. powyżej, na bieżąco dba by dane osobowe były usuwane w razie ustania ich przydatności do celu przetwarzania, a także m.in. w razie skutecznego zgłoszenia sprzeciwu lub żądania „bycia zapomnianym” przez osobę, której dane dotyczą.
- 6.3.** Wszystkie działania, o których mowa pkt. 6. będą stosowane do wszystkich nośników danych – zarówno elektronicznych (w tym backupów danych), jak i w formie wydruków, przetwarzanych przez PSS oraz podmioty przetwarzające dane dla PSS (w trybie art. 28 RODO). Odpowiednie umowy z podmiotami przetwarzającymi dane osobowe dla PSS w trybie art. 28 RODO uprawniają PSS do żądania podjęcia analogicznych działań również przez te podmioty.
- 6.4.** Oprogramowanie służące do przetwarzania danych osobowych w PSS posiada narzędzia umożliwiające spełnienie wymogów RODO, w szczególności w zakresie wyszukiwania danych osobowych, ich zmiany, generowania informacji dla uprawnionych i skutecznego usunięcia.

7. Opinia w przedmiocie istnienia obowiązku powołania inspektora ochrony danych osobowych, na podstawie art. 37 RODO

PSS rozważyła istnienie obowiązku powołania inspektora ochrony danych osobowych i uznała, że **nie dotyczy jej ten obowiązek**. Podejmując tę decyzję kierowała się tym, że:

- 7.1.** PSS nie jest organem ani podmiotem publicznym.
- 7.2.** Główna działalność PSS nie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10. RODO. Jedynym zbiorem danych osobowych, w skład którego wchodzi dane tej kategorii, jest zbiór danych osobowych pracowników. Gdyby przetwarzanie danych osobowych szczególnych kategorii co do własnych pracowników administratora stanowiło o spełnieniu przesłanki z art. 37 ust. 1 lit. c. RODO – w takim wypadku wielu pracodawców w UE byłoby zobowiązanych wyznaczyć inspektora ochrony danych z

tylko z tego powodu, że zatrudniają pracowników (co jest nie do pogodzenia z charakterem tego przepisu i prowadziło by do jego absurdalnej wykładni).

- 7.3. Główna działalność PSS nie polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę².

8. Opinia w przedmiocie istnienia obowiązku stworzenia i prowadzenia oceny ryzyka przetwarzania danych osobowych, na podstawie art. 35 i 36 RODO

- 8.1. PSS rozważyła stworzenie i prowadzenia oceny skutków przetwarzania danych osobowych i uznała, że **nie dotyczy jej ten obowiązek**. Dokonując tego ustalenia wzięto pod uwagę w szczególności to, że operacje przetwarzania dokonywane przez PSS:

8.1.1. nie są operacjami, które wchodzą w zakres wskazany w art. 35. ust. 3. RODO;

8.1.2. nie są operacjami, które wskazał Generalny Inspektor Ochrony Danych Osobowych w „Proponowanym wykazie rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych”, a który to wykaz dostępny był w maju 2018 roku na stronie: <https://www.giodo.gov.pl/pl/1520281/10430>;

8.1.3. nie są operacjami, które wskazała Grupa Robocza art. 29 na stronie 13. i 14. „Wytycznych dotyczących oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679” jako takie dla których istnieje prawdopodobieństwo, że wymagane będzie przeprowadzenie oceny skutków przetwarzania;

8.1.4. zgodnie z Wytycznymi dotyczącymi oceny skutków dla ochrony danych oraz pomagającymi ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679 przygotowanymi przez Grupę Roboczą art. 29 nie spełniają kryteriów wskazanych w tych wytycznych, a to:

8.1.4.1. **Ocena lub punktacja**, w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą” (motywy 71 i 91).

Jedynie operacja analizy CV przesłanych przez kandydatów do pracy w PSS spełnia to kryterium. Nie spełnia jednak żadnego z pozostałych kryteriów, co pozwala w ocenie PSS uznać, że nie wymaga ona przeprowadzenia oceny skutków przetwarzania³.

² W szczególności monitoring wizyjny stosowany w PSS nie wykorzystuje elementów rozpoznawania cech lub właściwości obiektów, które znajdują się w monitorowanej przestrzeni, zaś obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa.

³ Zgodnie z Wytycznymi dotyczącymi oceny skutków dla ochrony danych oraz pomagającymi ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679 przygotowanymi przez Grupę Roboczą art. 29 (str. 13): „w większości przypadków administrator danych może uznać, że przetwarzanie spełniające dwa kryteria będzie wymagało przeprowadzenia oceny skutków dla ochrony danych.”

- 8.1.4.2. **Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku:** przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, wywołujących „skutki prawne wobec osoby fizycznej” lub decyzji, które „w podobny sposób istotnie na nią wpływają” (art. 35 ust. 3 lit. a).

Żadna z operacji nie spełnia tego kryterium.

- 8.1.4.3. **Systematyczne monitorowanie:** przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie” (art. 35 ust. 3 lit. c).

Żadna z operacji nie spełnia tego kryterium⁴.

- 8.1.4.4. **Dane wrażliwe lub dane o charakterze wysoce osobistym:** obejmują szczególne kategorie danych osobowych określone w art. 9 (np. informacje o poglądach politycznych obywateli) oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10 RODO, a także inne dane wrażliwe zgodne z powszechnym rozumieniem tego terminu, czyli powiązane z gospodarstwem domowym i działalnością prywatną lub dotyczące wykonania prawa podstawowego (np. dane o lokalizacji mają związek z prawem do swobodnego poruszania się), lub dane których naruszenia może mieć wyraźny wpływ na codzienne życie osoby, której one dotyczą (np. dane finansowe, które mogą zostać wykorzystane do oszustw płatniczych).

Żadna z operacji nie spełnia tego kryterium oprócz operacji dotyczących pracowników i członków ich rodzin, przy czym nie przetwarza się danych o charakterze wysoce osobistym, a jedynie np. dane związane ze stanem zdrowia na potrzeby zabezpieczenia społecznego (zwolnienia lekarskie, tzw. L-4), przetwarzanie tych danych wynika wyłącznie z obowiązku nałożonego na PSS jako pracodawcę, przez przepisy prawa, które mają gwarantować pracownikowi prawo do świadczeń z ubezpieczeń społecznych.

- 8.1.4.5. **Dane przetwarzane na dużą skalę:**

Żadna z operacji nie spełnia tego kryterium.

- 8.1.4.6. **Dopasowywanie lub łączenie zbiorów danych** np. pochodzących z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.

Żadna z operacji nie spełnia tego kryterium.

4

W szczególności monitoring wizyjny stosowany w PSS nie wykorzystuje elementów rozpoznawania cech lub właściwości obiektów, które znajdują się w monitorowanej przestrzeni, zaś obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa.

8.1.4.7. **Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą:** przetwarzanie tego rodzaju danych stanowi jedno z kryteriów ze względu na zwiększoną nierównowagę sił między osobami, których dane dotyczą, a administratorem danych, co oznacza, że osoby fizyczne mogą mieć trudności z wyrażeniem zgody na przetwarzanie swoich danych lub z wyrażeniem sprzeciwu wobec ich przetwarzania, lub mogą mieć trudności z korzystaniem z przysługujących im praw. Do osób wymagających szczególnej opieki, których dane dotyczą, można zaliczyć dzieci (można je uznać za niezdolne do świadomego i przemyślanego sprzeciwienia się przetwarzaniu danych lub do wyrażenia zgody na przetwarzanie danych), pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl lub osoby starsze, pacjenci itp.) oraz w każdej sytuacji, gdy można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem administratora.

Żadna z operacji nie spełnia tego kryterium oprócz operacji dotyczących pracowników.

8.1.4.8. **Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych,** takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu itd.

Żadna z operacji nie spełnia tego kryterium.

8.1.4.9. **Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy”** (art. 22 i motyw 91). Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu.

Żadna z operacji nie spełnia tego kryterium.

8.1.4.10. **Transgraniczne przekazywanie danych poza Unię Europejską** (zgodnie z Proponowanym wykazem rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych, dostępnym w kwietniu 2018 roku na stronie: <https://www.giodo.gov.pl/pl/1520281/10430>)

Żadna z operacji nie spełnia tego kryterium.

8.2. Pomimo, że operacje przetwarzania danych szczególnych kategorii dotyczących pracowników mogą spełniać jednocześnie dwa kryteria (dane wrażliwe i osoby szczególne chronione), to po dodatkowej analizie, popartej udostępnionym przez GIODO wzorem „Rejestru czynności przetwarzania danych” dostępnym w maju 2018 roku na stronie: <https://www.giodo.gov.pl/pl/1520281/10449>, PSS uznaje, że operacje polegające na przetwarzaniu danych osobowych pracowników w związku z ich zatrudnieniem, a w szczególności na potrzeby wykonania obowiązków pracodawcy wynikających z przepisów prawa, nie są podstawą do sporządzenia oceny skutków przetwarzania danych osobowych.

8.3. Zgodnie z art. 35 ust. 1. i 11. RODO oraz z wytycznymi Grupy Roboczej art. 29 i GIODO, w PSS na bieżąco analizuje się ryzyko przetwarzania danych osobowych i w razie potrzeby sporządza ocenę skutków przetwarzania dla odpowiednich operacji, gdy wystąpią ku temu podstawy, a zwłaszcza:

- 8.3.1. przed rozpoczęciem nowej operacji przetwarzania – w szczególności z użyciem nowych technologii – która ze względu na swój charakter, zakres, kontekst i cele może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych,
- 8.3.2. po wystąpieniu naruszenia ochrony danych osobowych,
- 8.3.3. po zmianie przepisów prawa, dotyczącej ochrony danych osobowych, jak też po wydaniu przez Grupę Roboczą art. 29 lub krajowy organ nadzorczy wytycznych dotyczących prowadzenia oceny skutków przetwarzania danych lub oceny ryzyka przetwarzania.

Załącznik nr 1
do Polityki ochrony danych osobowych
Zgłoszenie naruszenia ochrony danych osobowych

.....
(miejsowość, data, godzina)

.....
(pieczęć administratora danych)

Prezes Urzędu Ochrony Danych Osobowych

**ZGŁOSZENIE NARUSZENIA OCHRONY
DANYCH OSOBOWYCH**

Data naruszenia:	Godzina naruszenia:
Kto powiadomił o naruszeniu:	Data i godzina powiadomienia:
Lokalizacja naruszenia:	
Charakter naruszenia:	
Ilość osób:	Ilość wpisów danych osobowych:
Kategorie osób, których naruszenie dotyczy:	Kategorie wpisów, których naruszenie dotyczy:
Okoliczności naruszenia:	
Konsekwencje naruszenia:	
Środki zaradcze:	
Zastosowane:	Proponowane:
Środki w celu zminimalizowania negatywnych skutków:	
Dodatkowe informacje:	
Dane kontaktowe do osoby mogącej podać więcej informacji:	
Imię i nazwisko:	Stanowisko:
Adres e-mail:	Telefon:

W imieniu Podwawelskiej Spółdzielni Spożyców z siedzibą w Krakowie

.....
(podpis osoby upoważnionej do reprezentacji)

Załącznik nr 2
do Polityki ochrony danych osobowych
Raport z naruszenia ochrony danych osobowych

.....
(miejsowość, data)

.....
(pieczęć administratora danych)

RAPORT Z NARUSZENIA OCHRONY
DANYCH OSOBOWYCH

Data naruszenia:		Godzina naruszenia:	
Kto powiadomił o naruszeniu:		Data i godzina powiadomienia:	
Lokalizacja naruszenia:			
Ilość osób:		Ilość wpisów danych osobowych:	
Kategorie osób, których naruszenie dotyczy:		Kategorie wpisów, których naruszenie dotyczy:	
Okoliczności naruszenia:			
Przyczyny i przebieg naruszenia:			
Naruszone dane osobowe:			
Skutki i konsekwencje naruszenia:			
Podjęte działania zaradcze i naprawcze:			
Dodatkowe informacje:			
Dokonano zgłoszenia organowi:		Dokonano zawiadomienia osoby:	
TAK	NIE	TAK	NIE
Uzasadnienie takiej decyzji:		Uzasadnienie takiej decyzji:	
Czy nastąpiło opóźnienie w zgłoszeniu/zawiadomieniu:			
TAK	NIE	NIE DOTYCZY	
Uzasadnienie opóźnienia (jeśli dotyczy):			
Osoba koordynująca:			
Imię i nazwisko:		Stanowisko:	

W imieniu Podwawelskiej Spółdzielni Spożywców z siedzibą w Krakowie

.....
(podpis osoby upoważnionej do reprezentacji)

Załącznik nr 3
do Polityki ochrony danych osobowych
Ewidencja naruszeń ochrony danych osobowych

Lp.	Data	Godzina	Lokalizacja	Ilość osób	Kategorie osób	Ilość wpisów	Kategorie wpisów	Opis	Zawiad. organu	Zawiad. osoby	Uwagi
1.											
2.											
3.											
4.											
5.											
6.											
7.											
8.											