ZARZĄDZENIE NR 3/PD/2019
PREZESA I DYREKTORA SĄDU REJONOWEGO W ŚWIEBODZINIE
z dnia 9 KWIETNIA 2019r.

w sprawie wprowadzenia w życie aktualizacji Polityki Bezpieczeństwa Informacji
w Sądzie Rejonowym w Świebodzinie

Na podstawie 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)(Dz. Urzęd. Unii Europ. z dnia 04.05.2016 r. L 119/1), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000, z późn. zm.), rozporządzenia Rady Ministrów z dnia z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247, z późn. zm.) oraz w zw. z zarządzeniem Ministra Sprawiedliwości z dnia 27 czerwca 2012 r. w spawie wprowadzenia Polityki Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości i sądów powszechnych (Dz. Urz. Min. Spraw. z 2012 r. poz. 93) ***zarządzam***, co następuje:

§ 1

1. Wprowadzam do stosowania z dniem **24 kwietnia 2019r.** aktualizację „Polityki Bezpieczeństwa Informacji w Sądzie Rejonowym w Świebodzinie" zwaną Systemem Zarządzania Bezpieczeństwem Informacji (SZBI).
2. Na SZBI w Sądzie Rejonowym, o którym mowa w ust. 1 składają się poniższe dokumenty prowadzone w formie tradycyjnej i elektronicznej (T - forma tradycyjna, papierowa / E - forma elektroniczna):
   1) Polityka Bezpieczeństwa Informacji (PBI) - T/E
   2) Polityka Bezpieczeństwa Danych Osobowych (PBDO) - T/E
   3) Polityka Realizacji Praw Podmiotów Danych (PRPPD) - T/E
   4) Polityka Bezpieczeństwa Systemów Teleinformatycznych (PBST) - T/E
   5) Regulamin Użytkownika Systemów Teleinformatycznych (RUST) - T/E
   6) Instrukcja Klasyfikacji Informacji (IKI) - T/E
   7) Reguły Anonimizacji Informacji (RAI) - T/E
   8) Procedura Szyfrowania Plików (PSP) - T/E
   9) Metodyka Szacowania Ryzyka (MSR) - T/E
   10) Plan Postępowania z Ryzykiem (PPZR) - T/E
   11) Procedura Reakcji na Incydenty oraz Naruszenia Ochrony Danych Osobowych (PRINODO) - T/E

12) Procedura Oceny Skutków Przetwarzania dla Ochrony Danych Osobowych (POSPODO) - T/E
13) Plan Postępowania z Ryzykiem (PPZR) - E
14) Rejestr Czynności Przetwarzania Danych Osobowych (RCPDO) - E
15) Rejestr Naruszeń Ochrony Danych Osobowych (RNODO) - E
16) Rejestr Ocena Skutków Przetwarzania Danych Osobowych dla Czynności Przetwarzania (ROSPDOCP) - E
17) Rejestr Osób Upoważnionych do Przetwarzania Danych Osobowych - E

3. Dokumentacja w wersji elektronicznej jest dostępna w zasobach wspólnych sieci lokalnej Sądu Rejonowego w Świebodzinie, wersja papierowa u Dyrektora Sądu Rejonowego.

§ 2

1. Funkcję Inspektora Ochrony Danych (IOD) w Sądzie Rejonowym pełni Pan **Przemysław Kanikowski.**
2. Funkcję Zastępcy Inspektora Ochrony Danych (ZIOD) w Sądzie Rejonowym powierzam Pani **Anecie Dziewa.**
3. Funkcję Administratora Systemu Informatycznego (ASI) w Sądzie Rejonowym powierzam Panu: **Mateuszowi Kapituła.**
4. Funkcję Zastępcy Administratora Systemu Informatycznego (ZASI) w Sądzie Rejonowym powierzam Pani **Ewelinie Pazgrat.**
5. Funkcję Administratorów Grupy Zasobów/Administratora Grupy Informacji (AGZ/AGI) powierzam:
   a) Głównemu Księgowemu,
   b) Kierownikowi sekretariatu I Wydziału Cywilnego,
   c) Kierownikowi sekretariatu II Wydziału Karnego,
   d) Kierownikowi sekretariatu III Wydziału Rodzinnego i Nieletnich,
   e) Kierownikowi sekretariatu IV Wydziału Pracy,
   f) Kierownikowi sekretariatu V Wydziału Ksiąg Wieczystych,
   g) Kierownikowi sekretariatu VI Zamiejscowego Wydziału Karnego w Sulechowie,
   h) Kierownikowi sekretariatu VII Zamiejscowego Wydziału Ksiąg Wieczystych w Sulechowie,
   i) Kierownikowi I Zespołu Kuratorskiej Służby Sądowej wykonującego orzeczenia w sprawach karnych,
   j) Kierownikowi II Zespołu Kuratorskiej Służby Sądowej wykonującego orzeczenia w sprawach rodzinnych i nieletnich,
   k) Kierownikowi Oddziału Administracyjnego,
   l) Kierownikowi Oddziału Finansowego.

§ 3

1. Każdy pracownik Sądu przed dopuszczeniem do przetwarzania danych osobowych/informacji jest zobowiązany do zapoznania się z treścią dokumentacji SZBI, załącznikami 1-2 do niniejszego zarządzenia oraz stosowania zasad w nich zawartych.
2. Załącznik nr 1 stanowi wyciąg z przepisów prawa w zakresie bezpieczeństwa informacji i ochrony danych osobowych.
3. Załącznik nr 2 określa podstawowe zasady przetwarzania danych osobowych.

4. Potwierdzenie dopełnienia obowiązku o którym mowa w pkt. 1 następuje w formie podpisania „Oświadczenia pracownika o zapoznaniu się z SZBI", którego wzór stanowi załącznik nr 3 do niniejszego zarządzenia.
5. Oświadczenie, o których mowa w ust. 4 pozostaje w aktach osobowych pracownika.

§ 4

1. Nadzór nad realizacją postanowień niniejszego zarządzenia sprawuje IOD, a w zakresie systemów informatycznych przetwarzających dane osobowe/informacje ASI.
2. Za poprawne przestrzeganie całości procedur, składających się na SZBI odpowiedzialny jest IOD, a w zakresie teleinformatycznym ASI.

§ 5

Upoważnienia do przetwarzania danych osobowych oraz oświadczenia wydane na podstawie Zarządzenia, o którym mowa w § 6 zachowują moc obowiązującą do dnia ich wygaśnięcia lub cofnięcia przez IOD lub ZIOD, nie dłużej jednak niż do dnia **30 kwietnia 2019r.**

§ 6

Traci moc obowiązującą Zarządzenie Prezesa Nr 4/2014 z dnia 30 maja 2014r. w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji" w Sądzie Rejonowym w Świebodzinie.

§ 7

Zarządzenie wchodzi w życie z dniem podpisania, z mocą obowiązującą od dnia **24 kwietnia 2019r.**

Świebodzin, dnia 9 kwietnia 2019r.

Dyrektor
Sądu Rejonowego w Świebodzinie
Beata Paszkiewicz

Prezes
Sądu Rejonowego w Świebodzinie
Marta Nikiel-Rzadkowska

Wyciąg z przepisów prawa w zakresie bezpieczeństwa informacji i ochrony danych osobowych

1) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 z późn. zm.)

Art. 107 [Odpowiedzialność za bezprawne przetwarzanie danych osobowych]

1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

Art. 108 [Odpowiedzialność za utrudnianie prowadzenia kontroli]

Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

2) Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2018 r. poz. 419 z późn. zm.)

Art. 11 [Tajemnice przedsiębiorstwa]

1. Czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża lub narusza interes przedsiębiorcy.
2. Przepis ust. 1 stosuje się również do osoby, która świadczyła pracę na podstawie stosunku pracy lub innego stosunku prawnego - przez okres trzech lat od jego ustania, chyba że umowa stanowi inaczej albo ustał stan tajemnicy.
3. Przepisu ust. 1 nie stosuje się wobec tego, kto od nieuprawnionego nabył, w dobrej wierze, na podstawie odpłatnej czynności prawnej, informacje stanowiące tajemnicę przedsiębiorstwa. Sąd może zobowiązać nabywcę do zapłaty stosownego wynagrodzenia za korzystanie z nich, nie dłużej jednak niż do ustania stanu tajemnicy.
4. Przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

Art. 23 [Naruszenie tajemnicy]

1. Kto, wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informację stanowiącą tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Tej samej karze podlega, kto, uzyskawszy bezprawnie informację stanowiącą tajemnicę przedsiębiorstwa, ujawnia ją innej osobie lub wykorzystuje we własnej działalności gospodarczej.

3) Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (Dz. U. z 2018 r. poz. 917 z późn. zm.)

Art. 100 [Obowiązki pracownika]

§1. Pracownik jest obowiązany wykonywać pracę sumiennie i starannie oraz stosować się do poleceń przełożonych, które dotyczą pracy, jeżeli nie są one sprzeczne z przepisami prawa lub umową o pracę.

§2. Pracownik jest obowiązany w szczególności:

1) przestrzegać czasu pracy ustalonego w zakładzie pracy;
2) przestrzegać regulaminu pracy i ustalonego w zakładzie pracy porządku;
3) przestrzegać przepisów oraz zasad bezpieczeństwa i higieny pracy, a także przepisów przeciwpożarowych;
4) dbać o dobro zakładu pracy, chronić jego mienie oraz zachować w tajemnicy informacje, których ujawnienie mogłoby narazić pracodawcę na szkodę;
5) przestrzegać tajemnicy określonej w odrębnych przepisach;
6) przestrzegać w zakładzie pracy zasad współżycia społecznego.

4) Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 2017 r. poz. 2204 z późn. zm.)

Rozdział XXXIII. Przestępstwa przeciwko ochronie informacji

Art. 265 [Tajemnica państwowa]

§1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli „tajne" lub „ściśle tajne", podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§2. Jeżeli informację określoną w §1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§3. Kto nieumyślnie ujawnia informację określoną w §1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 266 [Tajemnica służbowa]

§1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.

§3. Ściganie przestępstwa określonego w §1 następuje na wniosek pokrzywdzonego.

Art. 267 [Nielegalne uzyskanie informacji]

§1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w §1-3 ujawnia innej osobie.

§5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Art. 268 [Niszczenie informacji]

§1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2. Jeżeli czyn określony w §1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§3. Kto, dopuszczając się czynu określonego w §1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§4. Ściganie przestępstwa określonego w §1-3 następuje na wniosek pokrzywdzonego.

Art. 268a [Szkoda w bazach danych]

§1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§2. Kto, dopuszczając się czynu określonego w §1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§3. Ściganie przestępstwa określonego w §1 lub 2 następuje na wniosek pokrzywdzonego.

Art. 269 [Sabotaż komputerowy]

§1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§2. Tej samej karze podlega, kto dopuszcza się czynu określonego w §1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269a [Zakłócanie pracy w sieci]

Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269b [Bezprawne wykorzystanie programów i danych]

§1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 §1 pkt 4, art. 267 §3, art. 268a §1 albo §2 w związku z §1, art. 269 §1 lub 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§1a. Nie popełnia przestępstwa określonego w § 1, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia.

§2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

Art. 269c [Niepodleganie karze]

Nie podlega karze za przestępstwo określone w art. 267 §2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Załącznik nr 2 do Zarządzenia Nr 3/PD/2019
z dnia 9 kwietnia 2019r.

Podstawowe zasady przetwarzania danych osobowych

1) **Zasada zgodności z prawem, rzetelność i przejrzystość przetwarzania danych osobowych** - zgodnie z którą dane osobowe są przetwarzane w sposób zgodny z prawem (legalny) - na podstawie i granicach powszechnie obowiązujących przepisów prawa.
2) **Zasada ograniczenia celu przetwarzania danych osobowych** - zgodnie z którą dane osobowe są przetwarzane tylko w ściśle określonych celach, wynikających z powszechnie obowiązujących przepisów prawa oraz w przypadku procesów rekrutacji i Internetowego Portalu Informacyjnego Sądu Rejonowego na podstawie udzielonej przez podmiot danych zgody.
3) **Zasada minimalizacji pobieranych danych osobowych** - zgodnie z którą pobierana jest tylko taka ilość danych, która jest niezbędna, aby realizować podstawowe zadania Sądu Rejonowego w zakresie sprawowania wymiaru sprawiedliwości.
4) **Zasada prawidłowości pobieranych danych osobowych** - zgodnie z którą dane osobowe będą przetwarzane w sposób prawidłowy i w razie potrzeby uaktualniane, jeżeli dane osobowe są nieprawidłowe należy je niezwłocznie usuwać czy dokonywać sprostowania.
5) **Zasada ograniczenia przechowywania danych osobowych** - zgodnie z którą dane osobowe są przechowywane w formie umożliwiającej identyfikację danych osobowych przez okres nie dłuższy, niż jest to niezbędne do celów, dla których zostały pierwotnie pozyskane od podmiotu danych.
6) **Zasada integralności i poufności przetwarzania danych osobowych** - zgodnie z którą dane osobowe są przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem ich przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych i organizacyjnych.
7) **Zasada rozliczalności przetwarzania danych osobowych** - zgodnie z którą każdy pracownik Sądu Rejonowego jest odpowiedzialny za przestrzeganie wszystkich ww. zasad ochrony danych osobowych i musi być w stanie wykazać ich przestrzeganie w swojej codziennej pracy.
8) **Zasada pseudonimizacji i szyfrowania danych osobowych** - zgodnie z którą uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności podmiotów danych każdy pracownik Sądu Rejonowego stosuje odpowiednie środki techniczne i organizacyjne, aby zapewnić właściwy stopień bezpieczeństwa danym osobowym, np. szyfrowania i pseudonimizowania.
9) **Zasada niezwłocznego reagowania na incydenty fizyczne i techniczne związane z danymi osobowymi** - zgodnie z którą każdy pracownik Sądu Rejonowego będzie niezwłocznie zgłaszał wszelkie incydenty związane z danymi osobowymi do IOD lub ZIOD albo ASI lub ZASI, zgodnie z przyjętą w Sądzie Rejonowym dokumentacją SZBI.
10) **Zasada przetwarzania przez pracownika Sądu Rejonowego danych osobowych wyłącznie na polecenie administratora danych (Sądu Rejonowego)** - zgodnie z którą każdy pracownik Sądu Rejonowego zobowiązany jest przetwarzać dane osobowe do który ma dostęp wyłącznie na polecenie Sądu Rejonowego, stosownie do nadanego w tym zakresie upoważnienia do przetwarzania danych osobowych oraz uprawnienia do przetwarzania danych osobowych w systemach teleinformatycznych.

Załącznik nr 3 do Zarządzenia Nr 3/PD/2019
z dnia 9 kwietnia 2019r.

Oświadczenie pracownika

Ja niżej podpisana/ny oświadczam, iż zapoznałam/em się z dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) Sądu Rejonowego w Świebodzinie i jest mi znana treść 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) (Dz. Urzęd. Unii Europ. z dnia 04.05.2016 r. L 119/1), ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 ze zm.).

1) Zobowiązuję się:
   a) zachować w tajemnicy dane osobowe oraz informacje chronione, do których mam dostęp w trakcie wykonywania swoich obowiązków służbowych, zarówno w czasie trwania stosunku pracy, jak i po jego ustaniu,
   b) zabezpieczyć dane osobowe oraz informacje chronione przed dostępem do nich osób nieupoważnionych, zabraniem przez osobę nieuprawnioną, przetwarzaniem niezgodnym z prawem oraz zmianą, utratą, uszkodzeniem, zniszczeniem lub nielegalnym ujawnieniem.
2) Świadoma/y odpowiedzialności porządkowej (pracowniczej) i karnej oświadczam, że dane osobowe, do których mam dostęp na podstawie udzielonych mi upoważnień do przetwarzania danych osobowych oraz przyznanych uprawnień do przetwarzania danych osobowych w systemach teleinformatycznych zobowiązuje się przetwarzać zgodnie z przepisami prawa i przyjętą w Sądzie Rejonowym dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji.

.....

(data, podpis osoby składającej oświadczenie)