RODO

Szkolenie cykliczne w obrębie utworzonego Systemu Zarządzania Bezpieczeństwem Informacji

21-22.10.2019 r. – Tychy

Wprowadzenie

- Szkolenie obejmuje zagadnienia związane z Przetwarzaniem i Ochroną Danych Osobowych;
- Celem szkolenia jest pomoc w zrozumieniu czym są dane osobowe i w jaki sposób należy bezpiecznie je przetwarzać;
- Szkolenie zostało stworzone w oparciu o aktualną Politykę Bezpieczeństwa stosowaną w **Rejonowym Przedsiębiorstwie Wodociągów i Kanalizacji w Tychach S.A.** oraz Ustawę o Ochronie Danych Osobowych i RODO a także jej aktualizacje;
- Szkolenie przeznaczone jest dla wszystkich Pracowników **Rejonowego Przedsiębiorstwa Wodociągów i Kanalizacji w Tychach S.A.**
- Szkolenie pomoże Ci zrozumieć:
  - Czym są dane osobowe;
  - Jakie kategorie danych osobowych są szczególnie chronione;
  - W jaki sposób bezpiecznie przetwarzać dane osobowe.

Część I

PODSTAWOWE ŹRÓDŁA PRAWA OCHRONY DANYCH OSOBOWYCH

Polski system ochrony danych osobowych – od dnia 25.05.2018

- Konstytucja RP art. 47 i 51;
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 7 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:
  - tzw. **„RODO” lub „Rozporządzenie Ogólne”;**
- Nowa ustawa o ochronie danych osobowych z dn. 10 maja 2018 r.;
- ”Pakiet wdrażający RODO” z dn. 4 maja 2019 r.

Część II

RODO - WPROWADZENIE

UODO z 1997 r.	RODO
• Zbiory danych osobowych; • Proste klauzule informacyjne; • Możliwość powołania ABI; • Dane wrażliwe; • Podmiot przetwarzający; • Podstawowe prawa osób, których dane są przetwarzane; • Kary wyłączenie teoretyczne (ograniczenie lub pozbawienie wolności) – w praktyce nie stosowane.	• Rejestr czynności przetwarzania; • Rozbudowane i zindywidualizowane klauzule informacyjne; • Obowiązek powołania IOD – zwiększenie rangi i uprawnień Inspektora; • Dane szczególne – szerszy zakres szczególnych (biometryczne, wizerunek); • Procesor – zwiększenie zakresu obowiązków dla procesora, np. obowiązek prowadzenia Rejestru kategorii przetwarzanych danych; • Szerszy zakres uprawnień osób, których dane są przetwarzane, w tym prawo do bycia zapomnianym; • Obowiązek raportowania incydentów, niektórych do organu nadzorczego, z zachowaniem terminu 72 godzin od wykrycia; • Rozszerzenie kar (w tym kary finansowe); • Uregulowanie kwestii profilowania; • Zwiększenie ochrony danych dzieci; • Ułatwienia dla grup kapitałowych, wspólnie przetwarzających dane.

Kto podlega RODO?

- RODO podlega każdy przedsiębiorca, który prowadzi działalność w UE;
- Dowolna forma prawna: spółka, jednoosobowa działalność gospodarcza;
- Odziały w UE firm, które maja swoje siedziby poza UE;
- Bez znaczenia narodowość osób, których dane są przetwarzane;
- Nie ma znaczenia to, gdzie są przetwarzane dane osobowe (gdzie znajdują się serwery);
- RODO nie znajduje zastosowania do działalności osobistej i domowej, np. wysyłka zaproszeń na uroczystość lub corocznych kart świątecznych.

Jakie czynności podlegają RODO?

Wszelkie operacje na danych osobowych takie jak:

- Zbieranie danych,
- Przechowywanie danych,
- Usuwanie danych,
- Przenoszenie danych,
- Opracowanie danych,
- Udostępnianie danych.

Wszelkie usługi związane z wykorzystywaniem danych, np. usługi kurierskie, niszczenie dokumentów, pośrednicy ubezpieczeniowi, agenci i biura podróż, usługi księgowe, bankowe itp.

Czym w świetle RODO są dane osobowe

To wszelkie informacje odnoszące się do **zidentyfikowanej** lub **możliwej do zidentyfikowania** osobie fizycznej.

Osobą zidentyfikowaną jest taka osoba, której tożsamość znamy, którą możemy wskazać spośród innych osób.

Osobą możliwą do zidentyfikowania jest taka osoba, której tożsamość nie znamy, ale możemy poznać, korzystając z tych środków, które posiadamy.

Przykłady:

- Osoba zidentyfikowana: pracownik, klient sklepu internetowego;
- Osoba możliwa do zidentyfikowania: potencjalny kontrahent, którego posiadamy tylko numer ewidencyjny w CEIDG; nadawca listu poleconego na podstawie numer przesyłki.

Czym w świetle RODO są dane osobowe

Dane osobowe to informacje o osobach fizycznych – osoby prawne nie mają danych osobowych. Ale uwaga – pracownicy osób prawnych mogą mieć dane osobowe, jak każda inna osoba fizyczna.

- informacja „Apteka Kowalski Sp. z o.o.” – nie stanowi danych osobowych tego podmiotu;
- informacja „ Jan Nowak, pracownik Apteka Kowalski Sp. z o.o.” – może stanowić dane osobowe Jana Nowaka.

Wyróżnia się dwie kategorie danych:

- tzw. dane osobowe zwykłe;
- dane szczególnej kategorii danych (pochodzenie etniczne i rasowe, poglądy polityczne, przekonania religijne i światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dot. zdrowia, seksualności i karalności).

Czym w świetle RODO nie są dane osobowe

Danymi osobowymi, nie będą:

- samodzielne dane o dużym stopniu ogólności, np.: nazwa miasta, nazwa ulicy, kolor włosów, wiek.
- nazwa spółki, przedsiębiorstwa lub fundacji;
- adres mailowy w domenie publicznej (nigdy nie ma 100% pewności, że pod adresem jan.nowak@wp.pl będzie ta konkretna osoba);
- Dane osób zmarłych (osoba zmarła nie jest osobą fizyczną);
- imię i nazwisko oraz rozmiar ubrania (są to informacje zbyt ogólne do zidentyfikowania konkretnej osoby);

Warto jednak zapamiętać, że kilka powyższych cech zestawionych ze sobą może wystarczyć w zidentyfikowaniu konkretnej osoby, wówczas takie dane będą danymi osobowymi.

Czym są dane osobowe szczególnych kategorii (tzw. „wrażliwe”)?

Art. 9 (źródło: RODO)

„Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, biometrycznych w celu jednoznaczego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby (...)

ww. nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków: (...) j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych“

Kto może przetwarzać dane osobowe?

Jeżeli jakiś przedsiębiorca przetwarza dane osobowe, to może to zrobić jeden z dwóch kategorii podmiotów:

- administrator danych,
- podmiot przetwarzający dane (procesor).

Administrator danych to podmiot, który decyduje o celach i sposobach przetwarzania danych. Innymi słowy, decyduje o tym, po co (cele) i jak (sposoby) wykorzystać dane osobowe.

Przykłady:

- pracodawca w stosunku do danych zatrudnionego;
- handlowiec w stosunku do klienta;
- korzystający z bazy danych (*provider* zewnętrznych usług informatycznych) jako narzędzie wspierające działalność informacyjną, handlową, księgową itp.

Kto może przetwarzać dane osobowe?

Przedmiot przetwarzający dane osobowe nie decyduje o celach i środkach przetwarzania danych – działa na podstawie umowy z administratorem danych. Administrator danych może bowiem albo sam przetwarzać dane, albo skorzystać z usług zewnętrznego podmiotu, który te dane będzie przetwarzał dla niego.

Przykłady:

- zewnętrzna obsługa BHP,
- zewnętrzny właściciel przestrzeni serwerowej lub kont pocztowych,
- podmiot zajmującym się niszczeniem i utylizacją dokumentów.

Administrator oraz Procesor danych to zawsze określony podmiot – np. spółka, a nie jego pracownik.

Natomiast dane osobowe faktycznie przetwarzają konkretne osoby fizyczne (pracownicy), którzy powinny posiadać odpowiednie upoważnienia do przetwarzania danych osobowych.

Kiedy można przetwarzać dane osobowe?

Dane osobowe można przetwarzać wyłącznie wtedy, gdy istnieje tzw. podstawa prawna.

Przykłady:

- 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 administratorze,
- przetwarzanie jest niezbędne do ochrony **żywotnych interesów** osoby, której dane dotyczą, lub innej osoby fizycznej;
- dobro publiczne.

zgoda – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli.

Zasady przetwarzania danych osobowych

Art. 5 RODO – Dane osobowe muszą być przetwarzane:

- **zgodność z prawem, rzetelność i przejrzystość** – dane powinny być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- **ograniczenie celu** – dane powinny być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów historycznych lub celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami;
- **minimalizacja danych** – dane powinny być adekwatne, stosowne oraz ograniczone, co niezbędne do celów, w których są przetwarzane;
- **prawidłowość** – (poprawności) – dane mają być 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.

Informacje obowiązkowe przy zbieraniu zgody

- O tożsamości administratora i o jego danych kontaktowych;
- O danych kontaktowych Specjalisty/Inspektora ds. Ochrony Danych Osobowych;
- O celach i podstawie przetwarzania danych, że jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora;
- O odbiorcach danych osobowych lub o kategoriach odbiorców;
- O ewentualnych przekazaniu danych do państwa trzeciego;
- O okresie czasu, przez który dane będą przetwarzane;
- O prawie do żądania od administratora do wglądu, ich sprostowania, usunięcia lub ograniczeniu przetwarzania, prawie przeniesienia i zapomnienia;
- O prawie wniesienia skargi do organu nadzorczego.

Informacje obowiązkowe przy zbieraniu zgody

- Przetwarzanie jest niezbędne do wykonania umowy np. sprzedaży;
- Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze np. księgi rachunkowe;
- Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią – np. skierowanie pozwu do sądu o zapłatę.

Prawnie uzasadnionym interesem realizowanym przez administratora danych jest także marketing jego towarów i usług. Ale uwaga – pewne formy kontaktu z osobami, których dane dotyczą wymagają zgody.

Zgody wymaga przesłanie informacji handlowej za pomocą środków komunikacji elektronicznej lub widomości SMS o treści reklamowej.

Część III

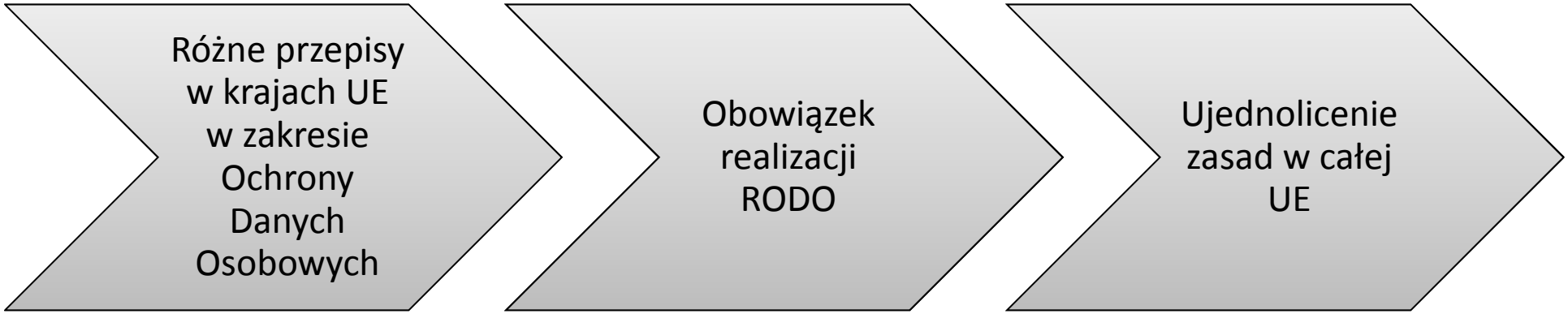
NOWE PRZEPISY – RODO – KARY

Dlaczego tak ważna jest ochrona danych?

Najistotniejszą informacją jest fakt, iż ochrona danych osobowych jest środkiem do realizacji prawa do prywatności.

W obecnych czasach informacje o danej osobie są rozpatrywane w kategoriach „produktu ekonomicznego“. Dane można zakupić oraz sprzedać.

Charakter zmian



Co grozi za naruszenie?

Kary wynikające z niedostosowania standardu zabezpieczenia informacji po 25 maja 2018 r., wynoszą do 4% całkowitego rocznego światowego obrotu grupy (lub 20 000 000,00 euro) oraz dodatkowo odszkodowania dla osób poszkodowanych naruszeniem **RODO** przez niedostosowany podmiot.

Kiedy możemy zostać ukarani?

- w przypadku kradzieży danych i niepoinformowaniu w czasie 72 godzin urzędu;
- w przypadku stwierdzenia w trakcie kontroli, że **administrator naruszył zapisy RODO**.

Domniemanie winy

RODO 5.2.

Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie.

RODO 82.3.

Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponosząc winy za zdarzenie, które doprowadziło do powstania szkody.

Rygor czasowy

Przedsiębiorstwo po 25 maja będzie musiało sprostać nieprzekraczalnym rygorom czasowym:

- 72 godziny na powiadomienie Urzędu Ochrony Danych Osobowych o naruszeniu ochrony danych osobowych;
- 1 miesiąc aby odpowiedzieć na żądania osoby dot. danych osobowych rzeczonej;
- 3 miesiące, aby spełnić żądania osoby, której dane dotyczą.

Tym samym: pracownicy **RPWiK Tychy S.A.** powiadamiają o incydencie bez zbędnej zwłoki **do 24 godzin od daty zdarzenia** (np. kradzieży pendrive'a).

Konsekwencje

Nieprzestrzeganie zasad określonych w PBDO stanowi naruszenie obowiązków pracowniczych, wynikających w szczególności z ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2018 r. poz.108, z późn. zm.):

- może wywoływać skutki dyscyplinarne i powodować pociągnięcie do odpowiedzialności, wynikającej z przepisów prawa;
- **uwaga!** obecnie z tytułu nie przestrzegania ochrony danych osobowych grozi **kara pozbawienia wolności od 1 roku do 3 lat**!

Co w przypadku naruszenia?

Co zrobić:

- procedura postępowania w przypadku naruszeń, w tym osoby odpowiedzialne, instrukcja postępowania w razie podejrzenie naruszeń (**załącznik: zgłoszenia naruszeń do administratora**) – dla całego personelu i przetwarzających;
- **dokumentowanie naruszeń** – dla celów dowodowych;
- wzory formularzy zgłaszania naruszenia ochrony danych osobowych do organu nadzorczego, do administratora w przypadku procesorów oraz do osób fizycznych;
- rejestr naruszeń i działań zaradczych.

Co w przypadku naruszenia?

Istotne jest również zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

Administrator zawiadamia osobę, **jasnym i prostym językiem**, jeżeli naruszenie ochrony danych osobowych może powodować **wysokie ryzyko** naruszenia jej praw lub wolności.

Wyjątki:

- administrator wdrożył środki uniemożliwiające nieuprawniony dostęp (szyfrowanie, etc.);
- administrator po naruszeniu zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia (*post factum* NDA, zdalne wyzerowanie, etc.);
- zawiadomienie wymagałoby niewspółmiernie dużego wysiłku **ale** wtedy obowiązek **publicznego komunikatu**.

Część IV

NOWE PRZEPISY – RODO – INTERPRETACJA PRAW I OBOWIĄZKÓW

Systematyka RODO

Dokument **RODO** można podzielić na następujące rozdziały:

0. Motywy

I. Przepisy Ogólne

II. Zasady

III. Prawa osoby, której dane dotyczą

IV. Administrator i podmiot przetwarzający

V. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

VI. Niezależne organy nadzorcze

VII. Współpraca i spójność

VIII. Środki ochrony prawnej, odpowiedzialność i sankcje

Najważniejsze założenia RODO

- bezpieczeństwo danych;
- legalność danych;
- prawa jednostki jeżeli chodzi o przechowywanie jej danych osobowych.

Jak podchodzić do danych osobowych?

Zgodnie z **RODO**, do danych osobowych podchodzimy:

- w konkretnym celu;
- przejrzyście, rzetelnie;
- z dbałością dotyczącą aktualności danych;
- bezpiecznie;
- adekwatnie (tylko tak długo ile potrzeba);
- adekwatnie (tylko tyle ile potrzeba);
- z ciągłą aktualizacją.

Adekwatne przetwarzanie danych

Dane osobowe muszą być zbierane w **konkretnych, jasnych i prawnie uzasadnionych celach.**

Nie mogą być również przetwarzane dalej w sposób niezgodny z tymi celami.

Prawidłowość danych

Dane muszą być przechowywane w **formie prawidłowej** oraz w razie potrzeby, **na bieżąco, uaktualniane.**

Dane osobowe, które są nieprawidłowe powinny zostać **niezwłocznie usunięte lub sprostowane.**

Zaleca się opracowanie procedury weryfikacji i zapewnienia jakości danych, w tym ich aktualizacji.

Ograniczenie przechowywania

Dane osobowe powinny być przechowywane w sposób umożliwiający identyfikację osoby, której dane dotyczą, przez okres **nie dłuższy niż jest to niezbędne** do celów, w których dane te są przetwarzane.

Dane osobowe można przechowywać dłużej w przypadkach gdy służą one do celów:

- archiwalnych w interesie publicznym;
- badań naukowych;
- historycznych;
- statystycznych.

Przechowywanie niewymagające identyfikacji

Jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do niniejszego rozporządzenia.

Jeżeli w przypadkach, o których mowa w ust. 1 niniejszego artykułu, administrator może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, w miarę możliwości informuje o tym osobę, której dane dotyczą. W takich przypadkach zastosowania nie mają art. 15-20, chyba że osoba, której dane dotyczą, w celu wykonania praw przysługujących jej na mocy tych artykułów dostarczy dodatkowych informacji pozwalających ją zidentyfikować.

Rejestr czynności przetwarzania danych

Administrator i Specjalista ds. Ochrony Danych Osobowych w przedsiębiorstwie prowadzą prosty **RCPD**, określający:

- cele przetwarzania danych;
- opis kategorii osób oraz kategorii danych osobowych;
- kategorie odbiorców danych;
- informacje o eksporcie danych;
- planowane terminy usunięcia kategorii danych;
- ogólny opis techniczny i organizacyjny środków bezpieczeństwa.

Jak podchodzić do danych osobowych?

Administrator jest odpowiedzialny za przestrzeganie przepisów i **musi być w stanie wykazać ich przestrzeganie.**

Jak podchodzić do danych osobowych?

- **Administrator** musi wykazać, że osoba wyraziła zgodę na przetwarzanie danych osobowych;
- Osoba może w każdej chwili wycofać zgodę na przetwarzanie jej danych, a procedura ta musi być równie łatwa i dostępna jak wyrażenie tej zgody;
- Zgoda ta musi być dobrowolna, to znaczy, że nie można jej wymuszać, np. przez wykonanie usługi.

Prawa osoby, której dane dotyczą

- prawo do informacji o zbieraniu danych;
- prawo dostępu do danych;
- prawo do kopii danych;
- prawo sprostowania i uzupełnienia;
- prawo do usunięcia danych (bycia zapomnianym);
- prawo do ograniczenia przetwarzania;
- prawo do przeniesienia danych;
- prawo sprzeciwu;
- prawo do ludzkiej interwencji;
- prawo do bycia obsłużonym (zakaz ignorowania);
- prawo do „czytelności” (opcja „ikonizacji”);
- prawo do ułatwiania (do przewodnika);

Prawa osoby, której dane dotyczą

- prawo do terminowości;
- prawo do nieprofilowania (sprzeciw „dowolny”);
- prawo do informacji o prawach;
- prawo do cofnięcia zgody;
- prawo do „równołatwości” niezgody;
- prawo do informacji o odbiorcach danych sprostowanych;
- opcja wygodnej elektronicznej obsługi praw;
- prawo do informacji o naruszeniu;
- prawo do skargi i do odwołania;
- prawo do odszkodowania;
- prawo do wsparcia organizacji społecznej.

Prawa osoby, której dane dotyczą

Administrator zobowiązany jest udzielić informacji dot. danych osobowych rzeczonej osobie, której te dane dotyczą w sposób:

- jasny;
- przejrzysty;
- łatwo zrozumiały;
- nieutrudniający.

Każdorazowa prośba skierowana dotycząca danych osobowych, skierowana do pracowników **RPWiK Tychy S.A.** powinna zostać niezwłocznie (**do 24 godzin**) przekierowana do **Inspektora Ochrony Danych Osobowych** (odo@rpwik.tychy.pl).

Prawa osoby, której dane dotyczą

Administrator danych osobowych (**RPWiK Tychy S.A.**) ma obowiązek komunikowania się z osobą zainteresowaną (której dotyczą rzeczone dane osobowe) w sposób:

- zwięzły;
- przejrzysty;
- zrozumiały;
- w łatwo dostępnej formie;
- jasnym i prostym językiem;
- w sposób ułatwiający osobie uzyskanie przysługujących jej praw.

Informacji można **tylko i wyłącznie** pisemnie (np. drogą elektroniczną), kierując interesanta do **Inspektora Ochrony Danych Osobowych** (odo@rpwik.tychy.pl).

Prawa osoby, której dane dotyczą

Administrator bez zbędnej zwłoki – a w każdym razie **w terminie miesiąca od otrzymania żądania** – udziela osobie, której dane dotyczą, informacji o podjętych działaniach.

W razie potrzeby termin ten można przedłużyć o **kolejne 2 miesiące** z uwagi na skomplikowany charakter żądania lub liczbę żądań.

Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to **niezwłocznie – najpóźniej w terminie miesiąca** od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Informacje oraz komunikacja i inne działania podejmowane **wolne są od opłat.**

Prawa osoby, której dane dotyczą

Osoba ma prawo do:

- potwierdzenia czy dane są przetwarzane;
- informacji jakie dane są przechowywane;
- dostępu do danych (kopia);
- informacji o celach przetwarzania danych;
- kategoriach przechowywanych danych;
- odbiorcach jej danych;
- źródle rzeczonych danych.

Jakich informacji może żądać osoba, której dane dotyczą?

- podania tożsamości oraz danych kontaktowych osobowy przetwarzającej jej dane w imieniu firmy;
- danych kontaktowych do Specjalisty ds. Ochrony Danych;
- informacji o odbiorcach danych osobowych;
- informacji o okresie przechowywania jej danych;
- sprostowania / uzupełnienia danych;
- usunięcia danych (prawo bycia zapomnianym).

Prawo kopii danych

Administrator dostarcza osobie kopię jej danych, która powinna być bezpłatna.

Na każdą kolejną kopię, o którą zwróci się osoba, której dane dotyczą, można 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.

Prawo sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od **administratora** niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.

Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Prawo do bycia zapomnianym

Prawo żądania niezwłocznego usunięcia dotyczących jej danych osobowych, jeżeli zachodzi jedna z następujących okoliczności:

- cofnięcie zgody;
- **sprzeciw** wobec przetwarzania **i nie występują nadrzędne prawnie uzasadnione podstawy** przetwarzania (np. przy marketingu bezpośrednim);
- dane były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego;
- **dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego** (jak przy marketingu bezpośrednim).

Prawo do ograniczenia przetwarzania

Osoba, której dane dotyczą, ma prawo żądania od **administratora** ograniczenia przetwarzania w następujących przypadkach:

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający **administratorowi** sprawdzić prawidłowość tych danych;
- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania.

Prawo do ograniczenia przetwarzania

- **administrator** nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie **administratora** są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą;
- gdy osoba kwestionuje prawidłowość danych osobowych (podlega weryfikacji);
- gdy jest to niezgodne z prawem;
- kiedy istnieje brak potrzeb przetwarzania.

Obowiązek powiadamiania

Administrator ma obowiązek poinformowania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagające niewspółmiernie dużego wysiłku.

Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Prawo do przenoszenia

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego **dane osobowe jej dotyczące, które dostarczyła administratorowi** oraz ma prawo przesłać te dane osobowe innemu **administratorowi** bez przeszkód ze strony **administratora**, któremu dostarczono te dane osobowe, jeżeli:

- przetwarzanie odbywa się na podstawie zgody lub umowy;
- w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały **przesłane przez administratora bezpośrednio innemu administratorowi**, o ile jest to technicznie możliwe.

Wyjątki: interes publiczny lub sprawowanie władzy publicznej powierzonej administratorowi.

Zautomatyzowane decyzje

Osoba, której dane dotyczą, ma prawo do tego, **by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu**, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Wyjątki: Powyższa zasada nie ma zastosowania, jeżeli ta decyzja:

- jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a **administratorem**;
- jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega **administrator** i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą;
- opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

Bezpieczeństwo

Dane osobowe muszą być 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”).

Bezpieczeństwo

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają **odpowiednie** środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa **odpowiadający** temu ryzyku, w tym:

- pseudonimizację i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, tzw. **CYBERBEZPIECZEŃSTWO**;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego – ***BCDR*** **(ang. *Business continuity and disaster recovery*)** .

Bezpieczeństwo

- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
- katalog środków bezpieczeństwa jest ogólny i ma charakter otwarty;
- ciężar ustalenia odpowiednich zabezpieczeń spoczywa na danej organizacji;
- każda organizacja (tj. nawet mały przedsiębiorca) przetwarzająca dane osobowe powinna stosować standardowe środki ochrony, takie jak: zobowiązania do zachowania poufności, programy antywirusowe, firewalle, szyfrowanie przenośnych nośników danych, kody dostępu do telefonów, kontrola dostępu, odpowiedni podział uprawnień, procedury aktualizacji oprogramowania,
- organizacyjne środki bezpieczeństwa powinny znaleźć odzwierciedlenie w odpowiednich politykach ochrony danych.

RODO istotne pojęcia

- Szyfrowanie;
- Pseudonimizacja;
- *Privacy by default*;
- *Privacy by design*.

Szyfrowanie

Wszędzie tam, gdzie można wyrządzić poważną szkodę jednostce lub szkoda może dotknąć dużą grupę osób, należy zastosować szczególne środki ochrony danych osobowych, w tym szyfrowanie danych.

Szyfrowanie **środek zabezpieczenia danych w tranzycie** (szczególnie przesyłanych siecią publiczną, emailem), jak i **danych w spoczynku** (czyli danych zapisanych na nośnikach – pendrive'ach, twardych dyskach, serwerach, kopiach zapasowych).

Oprócz poufności, szyfrowanie jest **podstawą zapewnienia autentyczności**. Autentyczność danych oznacza pewność, że pochodzą one od konkretnego autora i nie zostały zmienione. Autentyczność danych w systemach informatycznych zapewnia się poprzez podpis cyfrowy. Ten zaś oparty jest o szyfrowanie (asymetryczne).

Pseudonimizacja

„Pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Pseudonimizacja

Pseudonimizacja polega na zastępowaniu jednego atrybutu (z reguły atrybutu nietypowego ***[imię i nazwisko / PESEL]***) w zapisie innym atrybutem. W związku z tym **nadal istnieje prawdopodobieństwo pośredniego zidentyfikowania osoby fizycznej**; dlatego też stosowanie samej pseudonimizacji nie będzie skutkowało anonimowym zbiorem danych.

Pseudonimizacja dużych zbiorów danych to nietrywialne zadanie inżynierskie.

Privacy by default czyli minimalizacja danych

RODO 5.1.c. Dane osobowe muszą być: **(...) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane** („minimalizacja danych”).

RODO 25.2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

Privacy by design czyli projektowanie prywatności

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki techniczne i organizacyjne, takie jak **pseudonimizacja**, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak **minimalizacja** danych, oraz w celu nadania przetwarzaniu niezbędnych **zabezpieczeń**, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

Część V

NOWE PRZEPISY – RODO – OCHRONA DANYCH W RPWiK Tychy S.A.

Rozliczalność

„Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie”

Oznacza to tyle, że ciężar dowodu **zgodności obciąża przedsiębiorstwo**.

Wdrożenie i jego zgodność należy więc dobrze udokumentować. Istotne jest, aby zrobić to w **sposób łatwy do odtworzenia** (według określonej metodyki).

RODO podwaliny

RODO powstało na bazie normy **ISO 27001**, która jest jego dużo dokładniejszą, konkretniejszą i bardziej uszczegółowioną wersją.

Certyfikowanie z normy **ISO 27001** w 100% pokrywa zgodność z **RODO** i to właśnie oparcie się na tej normie gwarantuje rzetelne i poprawne wprowadzenie zmian w przedsiębiorstwie.

System pracy oraz zakres dokumentacji wdrożonej w Firmie: **RPWiK Tychy S.A.** jest zgodny z ww. grupą norm zarządzania jakością.

Norma PN ISO IEC 27001:2014

Uznawana międzynarodowo usystematyzowana metoda poświęcona bezpieczeństwu informacji:

- sterowany proces szacowania potrzeb wdrażania i utrzymywania systemu zarządzania BI;
- gotowy zbiór zabezpieczeń i najlepszych praktyk dotyczących BI;
- ma zastosowanie do wszystkich sektorów przemysłu;
- nastawiona na zapobieganie.

Definicje

Ryzyko - prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów.

Ryzyko szczątkowe - ryzyko, które pozostaje po wprowadzeniu zabezpieczeń.

Definicje

Zarządzanie ryzykiem - skoordynowane działania w celu kierowania i kontroli instytucji z uwzględnieniem ryzyka.

Postępowanie z ryzykiem - proces polegający na wyborze i wdrożeniu środków modyfikujących ryzyko.

Ryzyko inaczej - Oceń czy zabezpieczenia, które masz są adekwatne do tego co ci grozi.

Definicje

Informacja - dane przetworzone, czyli pogrupowane, poukładane i przefiltrowane w takich sposób, iż możliwe jest na ich podstawie podejmowanie decyzji biznesowych oraz wyciąganie wniosków.

Bezpieczeństwo informacji - ochrona informacji przed szerokim wachlarzem zagrożeń, w celu zapewnienia ciągłości biznesu, minimalizowania ryzyka biznesowego i maksymalizacji możliwości biznesowych.

Definicje

Istotna jest znajomość pojęć przez personel **RPWiK Tychy S.A.** W celu dalszego rozwoju przyjętego SZBI.

Wdrożony system jest tworem żywym i jego dalszy rozwój zależy w dużej mierze od zaangażowania kadry.

To w Państwa interesie leży kształtowanie go podług swoich potrzeb.

SZBI w RPWiK Tychy S.A.

RPWiK Tychy S.A. dbają o bezpieczeństwo informacji spełniając trzy główne warunki ochrony informacji:

- **poufność** - zapewnienie, że informacje są dostępne tylko i wyłącznie dla osób uprawnionych do ich dostępu;
- **integralność** - zagwarantowanie kompletności i dokładności informacji oraz metod ich przetwarzania;
- **dostępność** - zapewnienie upoważnionym osobom dostępu do informacji i związanych z nimi zasobów, zgodnie z określonymi potrzebami.

Zgody i informacje

- W ramach **RPWiK Tychy S.A.** zostały opracowane nowe wzory „klauzul informacyjnych” uwzględniające przy tym zasady transparentności;
- Opracowany został ponadto system przechowywania dowodów spełnienia obowiązku informacyjnego oraz posiadania zgód;
- Całość została ubrana w szeroko pojęty System Zarządzania Bezpieczeństwem Informacji zgodny z wymaganiami **RODO** w oparciu o metodykę pracy zgodną z wymaganiami ISO 2700x.

Integralność w RPWiK Tychy S.A.

Integralność to śledzenie procesu przetwarzania informacji we wszystkich formach występowania, po to aby uniemożliwić nieautoryzowaną modyfikację czy też wyeliminować niepoprawną metodę przetwarzania.

Innymi słowy **RPWiK Tychy S.A.** dbają o to, aby uniemożliwiona była umyślna lub nieumyślna nieautoryzowana zmiana informacji.

Dostępność w RPWiK Tychy S.A.

Dostępność to zapewnienie, iż informacja jest dostępna dla osoby uprawnionej zawsze gdy tego potrzebuje.

Utrata dostępności jako jednej z cech bezpieczeństwa informacji może prowadzić najczęściej do utraty ciągłości działania, a co się z tym wiąże produktywności. Może prowadzić do utraty przychodów, a także generować pośrednio bądź bezpośrednio straty finansowe.

RPWiK Tychy S.A. dbają o to, aby uprawnieni użytkownicy posiadali dostęp do konkretnej informacji w trybie ciągłym, w celu niwelacji ryzyka, że pracownicy, kierownicy, menedżerowie nie wykonają swoich prac na czas, lub po prostu zrezygnują z realizacji jakiegoś zadania, ponieważ skorzystanie z potrzebnych im zasobów okaże się niemożliwe.

Poufność w RPWiK Tychy S.A.

Najczęściej kiedy mówimy o bezpieczeństwie informacji w potocznym tego słowa znaczeniu, mamy na myśli przede wszystkim zachowanie poufności. Poufność oznacza zapewnienie, iż informacja jest dostępna wyłącznie dla osób uprawnionych, posiadających odpowiednie prawa dostępu.

Innymi słowy poufność rozumiana w **RPWiK Tychy S.A.** może być rozumiana jako zdolność do udostępniania informacji do wspólnego użytkowania przez wiele osób i jednocześnie **nieudostępniania jej tym osobom, które nie powinny się z daną informacją zapoznać**.

Dodatkowo zachowanie poufności ma uniemożliwić wykrycie źródła nadania, miejsca przeznaczenia danych, częstotliwości, długości i innych cech przesyłania.

Część VI

NOWE PRZEPISY – RODO – PRAKTYCZNA OCHRONA DANYCH W RPWiK Tychy S.A.

Ochrona danych w RPWiK Tychy S.A.

Obowiązki Administratorów Danych, w związku z RODO:

Art. 24 ust. 1 RODO

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, ***administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzane odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać****. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane*.

Co to oznacza w praktyce?

- Administrator Danych musi zdecydować o środkach technicznych i organizacyjnych, jakie wdroży;
- Administrator Danych musi zadbać o stały monitoring procesów związanych z przetwarzaniem;
- Administrator Danych musi zadbać o aktualizację zastosowanych środków;
- Administrator Danych odpowiada za skuteczność zastosowanych środków.

Ochrona danych w RPWiK Tychy S.A.

Metoda realizacji celu:

1. Wyznaczenie osoby odpowiedzialnej za wdrożenie, tj. Specjalisty ds. Ochrony Danych Osobowych;
2. Przeprowadzenie oceny stanu faktycznego – audyt systemu ochrony danych;
3. Wdrożenie odpowiednich rozwiązań organizacyjnych / proceduralnych;
4. Wdrożenie odpowiednich rozwiązań technicznych / zabezpieczeń fizycznych;
5. Wdrożenie odpowiednich rozwiązań informatycznych.

Zrealizowane zadania

- wysłany mailing do wszystkich kooperantów z klauzulą informacyjną dot. przetwarzania danych osobowych;
- spełnienie obowiązku informacyjnego za pośrednictwem strony internetowej;
- uruchomienie specjalnego adresu email na stronie RPWiK Tychy S.A. na który można zgłaszać wszelkie informacje dot. przetwarzania danych osobowych tj. odo@rpwik.tychy.pl;
- wprowadzona procedura rekrutacji**;**
- nowe wzory upoważnienia na przetwarzanie danych osobowych dla pracowników;

Zrealizowane zadania organizacyjne

- **wdrożenie dokumentacji ogólnej (procedury, regulaminy, instrukcje, polityki);**
- wdrożenie dokumentacji zgodnej z RODO (Rejestr czynności przetwarzania, Rejestr kategorii przetwarzanych danych, Analiza ryzyka, Ocena skutków dla przetwarzania, dokumentacja SZBI);
- cykliczne szkolenia pracowników;
- Powołanie Inspektora Ochrony Danych, prawidłowe umiejscowienie go w strukturze organizacyjnej;
- monitorowanie procesów związanych z przetwarzaniem danych;
- procedury postępowania z danymi zebranymi w terenie.

Zalecenie fizyczne

Przykładowe rozwiązania fizyczne do zastosowania w miejscach przetwarzania danych osobowych (częściowo zrealizowane):

- polityka postępowania z kluczami (kasetki, sejfy);
- zasada czystego biurka;
- alarmy, ochrona, monitoring;
- systemy antywłamaniowe;
- systemy przeciwpożarowe;
- zamykane szafy;
- kontrola dostępu do pomieszczeń, ograniczony dostęp.

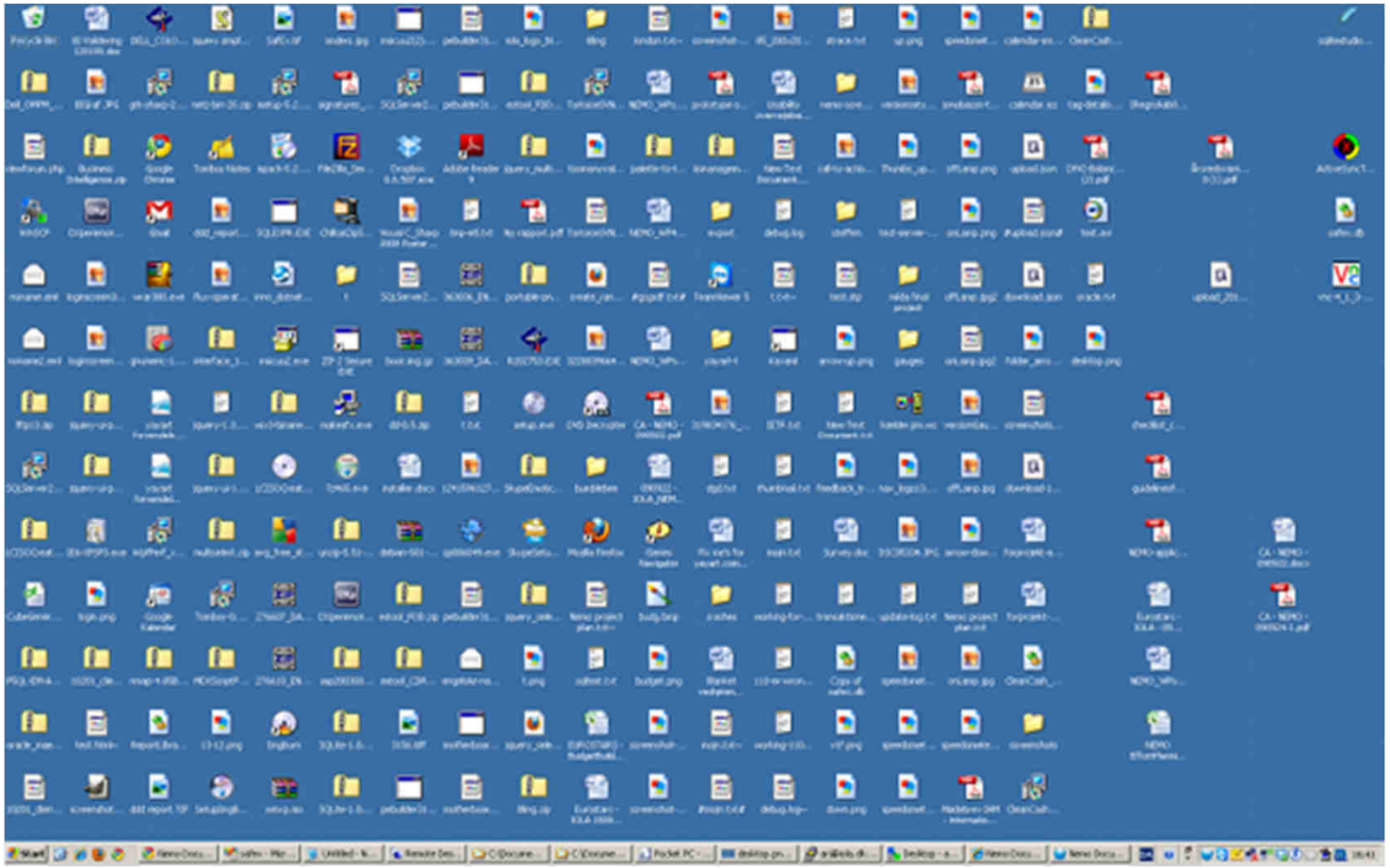
Poczta elektroniczna

Poczta elektroniczna stanowi podstawową broń w arsenale cyberprzestępców – jest narzędziem do wysyłania spamu, wirusów oraz przeprowadzania ataków *phishingowych*.

Właściwe korzystanie z poczty elektronicznej wiąże się z umiejętnością zabezpieczenia komputera przed działaniami przestępców oraz eliminacji zagrożeń pochodzących z zewnątrz, do których należą:

- spam, czyli niezamawiane wiadomości zawierające m.in. reklamy różnych usług i produktów;
- złośliwe oprogramowanie, czyli wirusy, trojany, *rootkity*, *scareware*, *ransomware* przesyłane w postaci załączników do e-maili lub pobierane po kliknięciu w odnośnik zawarty w wiadomości pochodzącej od przestępcy;
- *phishing*, czyli atak, którego celem jest wyłudzenie poufnych danych użytkownika poczty e-mail.

Praca na nieustrukturyzowanych danych



Praca na nieustrukturyzowanych danych

- O ile w programach komputerowych które wykorzystują bazy danych, łatwiej jest utrzymać „porządek” (z małymi wyjątkami). To dane nieustrukturyzowane mogą wyglądać tak jak na poprzednim slajdzie.
- Przyjęty system porządkowania plików (zwłaszcza zdanymi osobowymi) może ułatwić „poszukiwania”
- Pod rządami RODO, możemy natknąć się na konieczność realizacji takich poszukiwań do spełnienia prawa do bycia zapomnianym.
- Nie trzymamy plików „na zawsze” bo się może przydać (możemy ale zanonimizowane – bez danych osobowych).

Praca z wydrukami / kserokopie

Drukujemy i kopiujemy, coraz więcej.

- pilnujemy wydruków i kopii (w przypadku kiedy wydruki i kopie przekazujemy poza biuro warto prowadzić „rejestr” takich udostępnień. (co, gdzie, kiedy, komu, jaki cel) wtedy będzie to pod kontrolą.
- jak za dużo / nie potrzebne to:
    - recykling (jak nie zawiera danych osobowych);
    - niszczarka (jak są to dane osobowe).

Pamięci przenośne

Jeśli zdarzy się że musimy przenieść pliki pomiędzy obszarami przetwarzania to zadbajmy o ich bezpieczeństwo:

- albo nagrajmy je na pamięć USB szyfrowaną;
- albo skorzystajmy z programu szyfrującego dane;
- albo chociaż zróbmy sobie zaszyfrowane archiwum.

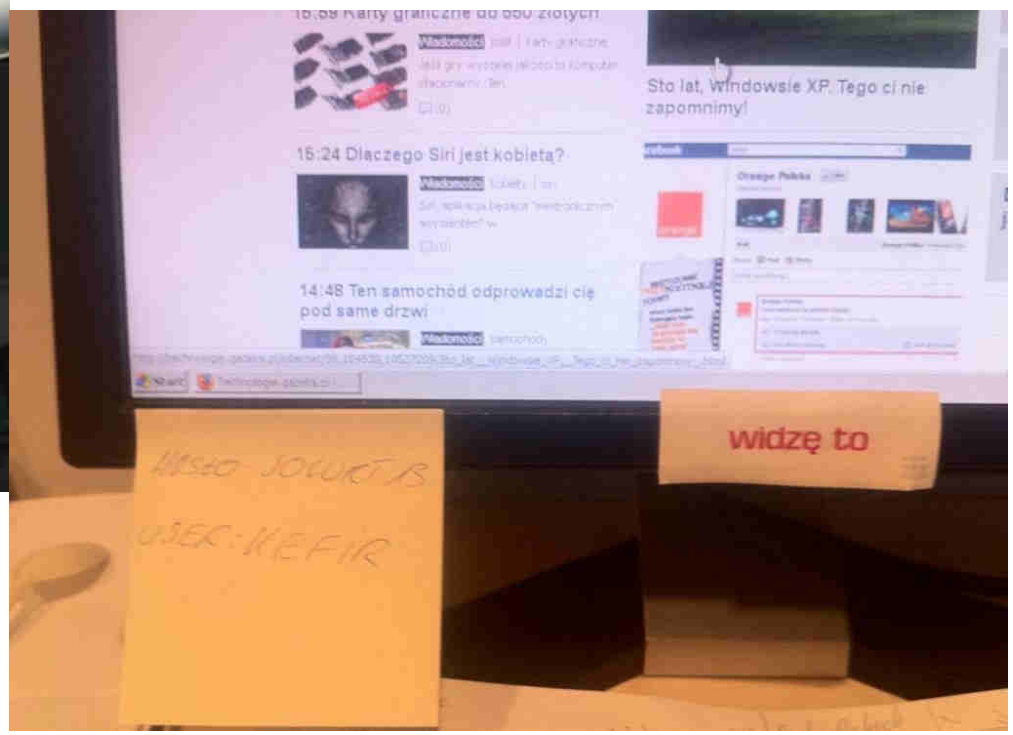
Zapisy umowne, wzory klauzul, upoważnień

Każdorazowo, w przypadku nowej zawieranej umowy, powinna ona zawierać zapisy w zakresie ochrony danych osobowych.

Wzory umów przechowywane są u **Inspektora Ochrony Danych Osobowych**.

Inspektor Ochrony Danych Osobowych, każdorazowo powinien być zaangażowany w prace nad warunkami współpracy z kooperantami.

Nieudostępnianie loginów i haseł do systemów



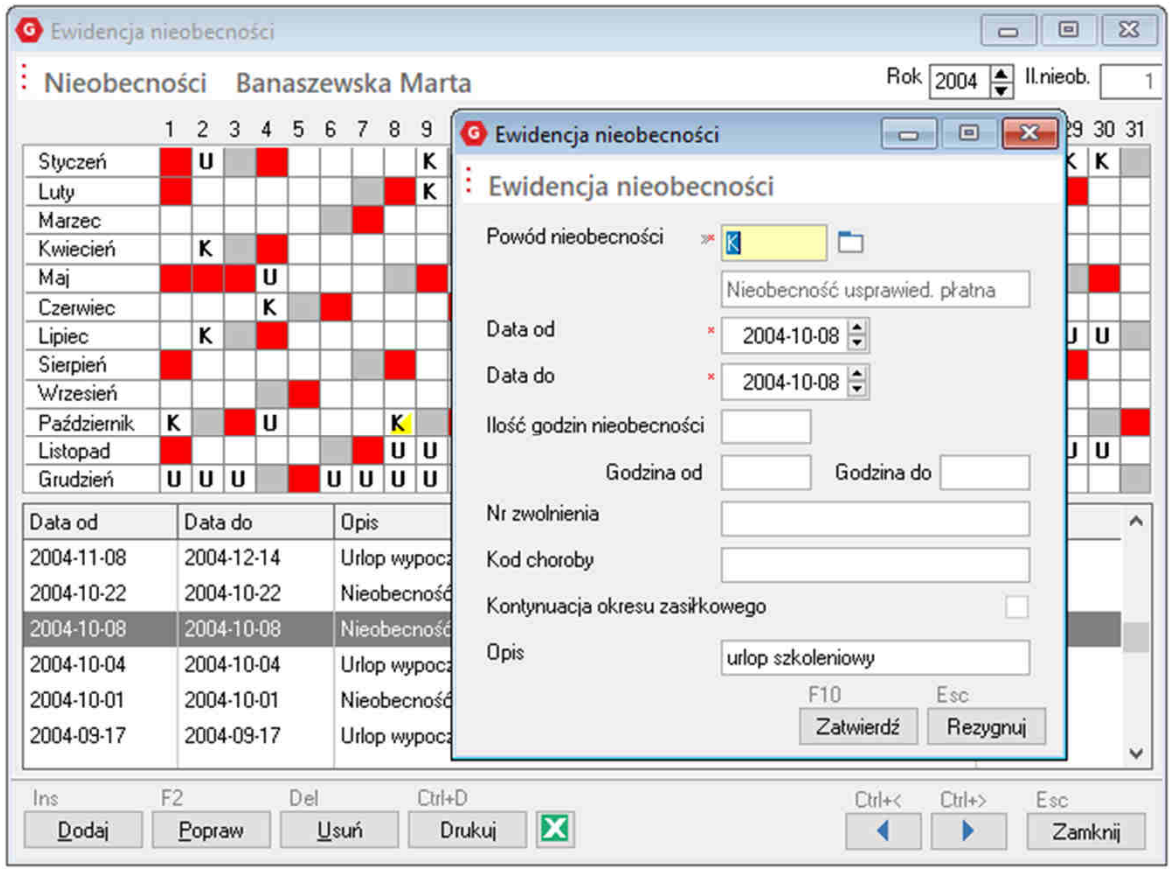
Polityka Bezpieczeństwa Teleinformatycznego

- Zgodnie z paragrafem 12 PBT w RPWIK Tychy S.A. zabronione jest:
  - **udostępnianie identyfikatorów i haseł osobom postronnym;**
  - łamanie haseł;
  - dokonywanie włamań na konta innych użytkowników;
  - nieprawne uzyskiwanie dostępu do kont administracyjnych;
  - zakłócanie działania usług;
  - omijanie zabezpieczeń (nie dotyczy audytu lub testowania);
  - rozprowadzanie wirusów, robaków i koni trojańskich oraz niechcianej poczty (spam);
  - praca na koncie innego użytkownika, za wyjątkiem sytuacji, w których wymagają tego prace konserwacyjne;
  - podejmowanie innych działań, mogących być zagrożeniem dla systemu.

Regulamin Ochrony Danych Osobowych

- Zgodnie z paragrafem 17 RODO w RPWIK Tychy S.A., każdy użytkownik jest zobowiązany do:
  - zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
  - niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
  - niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu Informatycznego;
  - poinformowania Administratora Systemu Informatycznego oraz IOD o podejrzeniu lub rzeczywistym ujawnieniu hasła;
  - stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych,
  - stosowania haseł nie posiadających w swojej strukturze części loginu,
  - stosowania haseł nie będących zbliżonymi do poprzednich (np. RPWiK2018 - RPWiK2019),
  - zmiany wykorzystywanych haseł nie rzadziej niż raz na 90 dni.

Informacje na listach obecności



Część VII

ZMIANY PO 4 MAJA 2019

4 maja 2019 roku w życie weszła **Ustawa z dnia 21 lutego 2019 r.** o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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).

Wyżej wymieniona **Ustawa spowodowała zmiany w prawie 170 obowiązujących ustawach**, z czego najważniejsze zmiany dotyczą **Kodeksu pracy.**

Zakres zbieranych danych od kandydata

Zgodnie z art. 22^1 § 1 KP, RPWiK Tychy S.A. ma prawo żądać od osoby ubiegającej się o zatrudnienie (kandydata) podania następujących danych osobowych:

- imienia (imion) i nazwiska;
- daty urodzenia;
- danych kontaktowych wskazanych przez kandydata;
- wykształcenia;*
- kwalifikacji zawodowych;*
- przebiegu dotychczasowego zatrudnienia.*

* Jeżeli rekrutacja na dane stanowisko pracy wymaga podania powyższych danych

Zakres zbieranych danych od pracownika

Zgodnie z art. 22^1 § 3 KP, RPWiK Tychy S.A. ma prawo żądać od pracownika podania dodatkowo danych osobowych obejmujących:

- adres zamieszkania;
- numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość;
- inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy;
- wykształcenie i przebieg dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie;
- numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.

Zakres zbieranych danych

Wszystkie dane osobowe, które pracodawca otrzymuje zarówno od osób starających się o zatrudnienie (kandydatów do pracy), jak również pracowników, przekazywane są w formie oświadczenia.

W związku z powyższym, zabrania się zbierania kserokopii dokumentacji potwierdzającej dane osobowe.

Kandydat do pracy lub pracownik może zostać poproszony o potwierdzenie autentyczności swoich danych osobowych, jednakże pracodawca może otrzymać dokumenty potwierdzające dane osobowe tylko i wyłącznie do wglądu.

Podstawa prawna przetwarzania danych osobowych

Jeżeli kandydat do pracy dostarcza w swoim CV jedynie informacje, które wymagane są przepisami Kodeksu pracy, to podstawę do ich przetwarzania stanowi art. 6 ust. 1 lit. c) RODO – obowiązek prawny ciążący na administratorze. Oznacza to, że do takiego CV kandydat nie musi dołączać stosownej klauzuli o zgodzie na przetwarzanie swoich danych osobowych.

Jeżeli kandydat do pracy dostarczy w swoim CV dodatkowe dane osobowe, które nie są wymagane, zgodnie z Kodeksem pracy, na etapie rekrutacji, to podstawę do ich przetwarzania stanowi art. 6 ust. 1 lit. a) RODO – zgoda osoby na przetwarzanie jej danych osobowych. W takiej sytuacji, jeżeli w CV nie znajduje się klauzula zgody na przetwarzanie dodatkowych danych osobowych, CV takiej osoby powinno być automatycznie usunięte.

Zgoda stanowi również podstawę na przetwarzanie danych osobowych kandydata do pracy w przyszłych procesach rekrutacyjnych.

Przetwarzanie dodatkowych danych osobowych

Pracodawca może przetwarzać dodatkowe dane o kandydatach do pracy oraz o swoich pracownikach, które nie są wymagane przepisami prawa. Dane te muszą być przekazane jednakże z inicjatywy kandydata lub pracownika. W związku z powyższym, pracodawca nie może narzucić obowiązku przekazania danych osobowych, jeżeli obowiązek ich przetwarzania nie wynika z przepisów prawa.

Dane biometryczne

Przetwarzanie danych biometrycznych pracownika jest dopuszczalne także wtedy, gdy podanie takich danych jest niezbędne ze względu na kontrolę dostępu do szczególnie ważnych informacji, których ujawnienie może narazić pracodawcę na szkodę, lub dostępu do pomieszczeń wymagających szczególnej ochrony.

Do przetwarzania tych danych mogą zostać dopuszczone jedynie osoby posiadające stosowne upoważnienie.

Część VIII

NOWE PRZEPISY – RODO – PODSUMOWANIE

Informacja jako wartość biznesowa

Informacje będące w posiadaniu organizacji mają swoją realną wartość, dlatego też są podatne na zagrożenia takie jak np.: kradzież, zafałszowanie, zniszczenie.

Czasy w których żyjemy dokładają do tego swoją “cegiełkę” w postaci coraz bardziej niebezpiecznej cyberprzestępczości. Włamania hakerów, kradzieże numerów kart kredytowych, szkodliwe i zawirusowane oprogramowanie.

Informacja jako wartość biznesowa

To wszystko grozi nie tylko utratą reputacji, zaufania firmy, konkurencyjności, ale także naraża przedsiębiorstwo na duże kary i straty finansowe.

W wielu instytucjach można zaobserwować wiele zdarzeń, które w skutek braku świadomości pracowników mogą doprowadzić do przekłamania, ujawnienia bądź utraty istotnych informacji. Przykładem tego są źle przetworzone lub obrobione dane (np. księgowe, finansowe, czy projektowe) zagubienia nośników z danymi (laptopy pendrive', płyty CD, karty pamięci flash), karteczki z hasłami przyklejone do monitora, ekrany monitorów zwrócone w stronę Klientów, dokumenty leżące na biurku, które mogą zostać zabrane przez osobę niepowołaną, dokumenty zawierające istotne informacje wyrzucone na śmietnik itp.

Informacja jako wartość biznesowa

W celu minimalizacji ryzyka utraty integralności, poufności oraz dostępności danych, **RPWiK Tychy S.A.** wprowadziły jasne i przejrzyste reguły powstałe na kanwie nowych przepisów w zakresie ochrony danych osobowych, takie jak:

1. **Politykę bezpieczeństwa informacji;**
2. **Procedury postępowania z danymi osobowymi (wielopłaszczyznowo);**
3. **Komplet klauzul o poufności – zarówno z kontrahentami jak i pracownikami;**

Oraz inne dokumenty towarzyszące.

Korzyści płynące z RODO

- **porządek** – uporządkowanie procesów, wyczyszczenie składzików, efektywność operacji;
- **orientacja na Klienta** – wymuszenie zwiększenia świadomości, narzędzia obsługi;
- **wymuszona dobra jakość danych** – problem z jakością danych utrudnia dotarcie do klientów z ofertą i dotarcie z dobrą ofertą do klientów;
- **łatwiej o dowody naruszeń wewnętrznych**;
- **lepsza ochrona danych**;
- **lepsza analiza danych nieustrukturyzowanych**;
- **szansa na konkurowanie zaufaniem i bezpieczeństwem**.

DZIĘKUJEMY ZA UWAGĘ