# Polityka Bezpieczeństwa Informacji Grupy Diagnostyka

## Cel Polityki

Grupa Diagnostyka dba o to, aby wszystkie spółki w Grupie stosowały te same zasady ochrony informacji.

W ramach tej polityki:

- Chronimy dane, które są objęte ochroną prawną. Dotyczy to szczególnie danych osobowych i medycznych, a także informacji handlowych, finansowych, technologicznych i związanych z zabezpieczeniami.
- Dbamy, aby wszystkie spółki zależne stosowały te same zasady bezpieczeństwa informacji.
- Chronimy informacje przed nieautoryzowanym dostępem, ujawnieniem, zmianą, usunięciem lub zniszczeniem.
- Uczymy pracowników, czym jest bezpieczeństwo informacji i jak o nie dbać.

## Zakres Polityki

Ta polityka dotyczy wszystkich spółek, które należą do Grupy Diagnostyka. Obowiązuje:

- pracowników,
- kontrahentów,
- współpracowników, którzy mają dostęp do danych i systemów Grupy.

Dotyczy to danych przechowywanych zarówno elektronicznie, jak i na papierze. Obejmuje też systemy do przesyłania i wymiany informacji.

## Definicje

W tym dokumencie używamy poniższych pojęć:

- **My** – oznacza firmę Diagnostyka S.A.
- **Informacje chronione** (**dane**) – to informacje, których ujawnienie może zaszkodzić Grupie. Należą do nich m.in.:
    - dane osobowe pacjentów, pracowników, kontrahentów i klientów,
    - informacje o zdrowiu pacjentów,
    - wyniki badań i konsultacji medycznych,
    - dokumentacja medyczna i rejestry medyczne,
    - dane o zatrudnieniu,
    - informacje handlowe (np. umowy),
    - informacje finansowe (np. dokumenty księgowe),
    - dane o technologii, której używamy,
    - informacje o naszych zabezpieczeniach (organizacyjnych, fizycznych i informatycznych).
- **Systemy informatyczne** – programy, urządzenia i sieci, które służą do przechowywania, przesyłania i przetwarzania danych w Grupie lub między Grupą a kontrahentami.

- **Spółki zależne** – firmy, które należą do Grupy Diagnostyka, w tym także Diagnostyka S.A.
- **Użytkownicy** – osoby, które mają dostęp do chronionych informacji. Na przykład: pacjenci, pracownicy, współpracownicy, partnerzy technologiczni.
- **Kontrahenci** – firmy lub organizacje, które świadczą usługi dla spółek należących do Grupy.
- **Sztuczna inteligencja (AI)** – technologie oparte na uczeniu maszynowym, które pozwalają komputerom analizować dane, rozpoznawać wzorce i podejmować decyzje.
- **Incydent bezpieczeństwa** – każde zdarzenie, które może zagrozić poufności, integralności lub dostępności chronionych informacji.
- **Grupa Diagnostyka (Grupa)** – cała grupa firm, która obejmuje Diagnostyka S.A., spółki zależne i inne spółki, w których Grupa ma udziały.
- **Właściciel biznesowy systemu** – pracownik odpowiedzialny za dany system informatyczny w firmie. Jego zadania to:
    - określanie, czego firma potrzebuje od systemu,
    - zarządzanie zasobami potrzebnymi do jego działania (np. budżetem, personelem, technologią),
    - dbanie, by system wspierał cele biznesowe firmy, był bezpieczny oraz zgodny z założeniami.

## Zasady bezpieczeństwa informacji

W tej części Polityki opisujemy podstawowe zasady, które obowiązują we wszystkich spółkach Grupy Diagnostyka:

- **Poufność** – spółki muszą chronić dane przed dostępem osób nieuprawnionych. Dotyczy to ich przechowywania, przesyłania i udostępniania. Każda spółka zależna musi dbać o to, by dane nie trafiły do osób, które nie mają do nich prawa.
- **Integralność** – dane nie mogą być zmieniane w sposób nieuprawniony. Zarząd każdej spółki odpowiada za to, by informacje były prawidłowo przechowywane i przetwarzane zgodnie z ustalonymi procedurami.
- **Dostępność** – dane muszą być dostępne wtedy, gdy są potrzebne – ale tylko dla osób uprawnionych, w tym pacjentów. Jeśli system informatyczny ulegnie awarii, spółka musi szybko zareagować i przywrócić jego działanie.
- **Zgodność z przepisami prawa** – wszystkie spółki Grupy muszą przestrzegać prawa dotyczącego ochrony danych osobowych i bezpieczeństwa informacji. Dotyczy to w szczególności:
    - RODO – Rozporządzenia UE 2016/679 o ochronie danych osobowych,
    - ustawy o ochronie danych osobowych,
    - oraz innych obowiązujących przepisów.

## Ochrona danych osobowych pacjentów

Spółki, które należą do Grupy Diagnostyka muszą przestrzegać zasad RODO, gdy przetwarzają dane pacjentów. Oznacza to, że:

- Spółki muszą przechowywać dane osobowe i medyczne pacjentów w bezpieczny sposób – zarówno elektronicznie, jak i na papierze.
- Dostęp do danych mogą mieć tylko osoby, które potrzebują ich, by wykonywać swoje obowiązki służbowe.
- Każda spółka powinna kontrolować, kto ma dostęp do danych pacjentów.

Jeśli przesyłamy dane lub nośniki danych (np. płyty, dyski, dokumenty) między spółkami Grupy albo do kontrahentów, musimy stosować odpowiednie zabezpieczenia, na przykład:

- szyfrowanie,
- połączenia VPN,
- bezpieczne koperty lub opakowania.

## Przechowywanie danych

W tej części Polityki opisujemy, jak spółki Grupy powinny przechowywać dane:

- **Dane muszą być dobrze zabezpieczone**:
  - Spółki muszą szyfrować dane elektroniczne oraz używać do tego aktualnych i bezpiecznych metod.
  - Spółki muszą przechowywać dane papierowe (fizyczne) w zamkniętych i chronionych miejscach – dostęp do nich mają tylko uprawnione osoby.
- **Rodzaj zabezpieczeń powinien zależeć od typu danych** – zgodnie ze standardami przyjętymi w Grupie Diagnostyka.
- **Dostęp do danych opiera się na zasadzie minimalnych uprawnień** – każdy użytkownik ma dostęp tylko do tych danych, które są mu potrzebne. Wyznaczona osoba w każdej spółce nadzoruje uprawnienia i regularnie je przegląda.
- **Dla każdej kategorii danych ustalony jest czas przechowywania** – znajdziesz go w *Polityce Klasyfikacji Informacji*.
- **Spółka usuwa niepotrzebne dane bezpiecznie i trwale** – np. nadpisuje dane na nośnikach losowymi ciągami zer i jedynek.
- **Spółka wycofuje i niszczy nośniki danych, które trzeba zniszczyć.** Zgodnie z procedurami.

## Wymiana danych między spółkami zależnymi

W tej części Polityki opisujemy zasady wymiany danych między spółkami zależnymi

- **Zasada minimum** – spółki mogą przekazywać sobie tylko te dane, które są naprawdę potrzebne do realizacji zadań.
- **Szyfrowanie danych** – wszystkie dane przesyłane między spółkami muszą być szyfrowane zgodnie z najlepszymi praktykami.
- **Umowy o poufności** – spółki zależne i kontrahenci muszą mieć podpisane umowy, które regulują zasady poufnej wymiany danych.

## Kontrola dostępu do informacji

Spółki Grupy muszą kontrolować, kto ma dostęp do informacji – zarówno w systemach informatycznych, jak i w budynkach:

- **Dostęp do systemów informatycznych** musi być nadawany zgodnie z zakresem obowiązków użytkownika.
- **Dostęp do miejsc fizycznych**, takich jak serwerownie, centra danych czy szafy dystrybucyjne, musi być ograniczony tylko do uprawnionych osób.
- **Hasła i logowanie**:

    - Użytkownicy muszą używać silnych haseł, zgodnych z przyjętym standardem.
    - W systemach, gdzie to możliwe, użytkownicy stosują uwierzytelnianie dwuskładnikowe (np. hasło + kod SMS lub aplikacja).
- **Zarządzanie dostępem**:
    - Każda spółka musi regularnie przeglądać i aktualizować dostęp użytkowników.
    - W spółkach muszą być określone jasne zasady przyznawania, zmiany i usuwania uprawnień.

## Zarządzanie ryzykiem

Spółki zależne Grupy Diagnostyka muszą aktywnie zarządzać ryzykiem, które dotyczy bezpieczeństwa informacji:

- Każdy właściciel biznesowy zasobu (np. systemu, danych) jest odpowiedzialny za bieżące monitorowanie ryzyka i dostosowywanie działań do zmieniających się zagrożeń.
- Każdy właściciel biznesowy regularnie ocenia i dokumentuje ryzyko – tak, by zapobiegać stratom i incydentom bezpieczeństwa.

## Ochrona fizyczna i infrastrukturalna

W tej części Polityki opisujemy zasady ochrony fizycznej i infrastrukturalnej:

- Spółki muszą fizycznie zabezpieczyć serwery, komputery i inne urządzenia, które przechowują dane chronione. Np. w zamkniętych pomieszczeniach, do których dostęp mają tylko uprawnione osoby.
- Miejsca, gdzie są dane chronione, muszą mieć techniczne środki ochrony – np. systemy kontroli dostępu.
- Spółki przyznają dostępy tylko tym osobom, które naprawdę ich potrzebują do pracy. W systemach kontroli dostępu musi być opcja, aby kto i kiedy miał dostęp do danego miejsca.

## Monitorowanie i audyt bezpieczeństwa informacji

W tej części Polityki opisujemy zasady monitorowania i audytu bezpieczeństwa informacji:

- Spółki zależne muszą monitorować dostęp do systemów informatycznych i zapisywać działania użytkowników.
- Spółki zależne muszą całodobowo monitorować bezpieczeństwo infrastruktury IT.
- Biuro Bezpieczeństwa będzie przeprowadzać regularne audyty bezpieczeństwa w Grupie.  Aby sprawdzić zgodność z politykami i wykrywać ewentualne problemy.
- Jeśli w systemach zostaną wykryte luki lub słabe punkty, spółki muszą je jak najszybciej usunąć – zgodnie z określoną procedurą zarządzania podatnościami.

## Eksploatacja systemów informatycznych

W tej części Polityki opisujemy zasady eksploatacji systemów informatycznych:

- Pracownicy mogą korzystać tylko z systemów informatycznych, które są zatwierdzone i zarejestrowane.
- Właściciel biznesowy każdego systemu musi przypisać mu poziom krytyczności – zależnie od tego:

    - jak ważne i wrażliwe dane są w nim przetwarzane,
    - jakie mogą być skutki braku dostępności danych,
    - jak system wspiera procesy biznesowe.
- Dla każdego systemu spółka wyznacza osoby odpowiedzialne za:
    - administrację systemem (administratorzy),
    - nadzór nad zadaniami administracyjnymi i zapewnienie potrzebnych zasobów (np. budżet, personel).
- Dyrektor IT definiuje, jakie dokładnie obowiązki mają administratorzy danego systemu.

## Bezpieczne korzystanie ze sztucznej inteligencji (AI)

W tej części Polityki opisujemy, jak bezpiecznie korzystać ze sztucznej inteligencji (AI):

- Jeśli pracownicy używają sztucznej inteligencji (AI) do przetwarzania danych osobowych lub medycznych, muszą przestrzegać przepisów o ochronie danych.
- Spółki muszą chronić dane, których używa AI, przed nieautoryzowanym dostępem – np. przez odpowiednie zabezpieczenia techniczne i organizacyjne.
- Tylko osoby z odpowiednimi uprawnieniami mogą mieć dostęp do systemów AI. Administratorzy systemów oraz ich przełożeni są odpowiedzialni za nadzór nad tym dostępem.
- Spółki muszą regularnie monitorować i audytować wykorzystanie AI. Żeby upewnić się, że pracownicy używają systemów bezpiecznie i zgodnie z zasadami.
- Zanim spółka wdroży system AI, właściciel biznesowy musi ocenić ryzyko – np. związane z prywatnością, bezpieczeństwem czy wpływem na organizację.
- Umowy z dostawcami AI muszą zawierać zapisy o bezpieczeństwie informacji i ochronie danych.
- Korzystanie z AI musi być zgodne z prawem, regulacjami oraz zasadami etycznymi.

## Procedury reagowania na incydenty bezpieczeństwa

W tej części Polityki opisujemy procedury reagowania na incydenty bezpieczeństwa:

- Jeśli dojdzie do naruszenia bezpieczeństwa informacji (np. wycieku danych, cyberataku), spółki zależne muszą natychmiast podjąć działania, by ograniczyć jego skutki.
- Reakcja spółek musi być zgodna z ustalonym **Procesem Obsługi Incydentów**.
- Spółki zgłaszają każdy incydent do Chief Security Officera Grupy. W razie potrzeby także do Inspektora Ochrony Danych Osobowych oraz odpowiednich służb.
- Po każdym incydencie spółki przeprowadzają analizę przyczyn i wprowadzają działania naprawcze.

## Szkolenia i budowanie świadomości cyber zagrożeń

W tej części Polityki opisujemy zasady szkoleń i budowania świadomości cyber zagrożeń:

- Biuro Bezpieczeństwa razem z Zespołem Komunikacji i EB regularnie informują pracowników o zagrożeniach i dobrych praktykach w zakresie bezpieczeństwa informacji.
- Pracownicy muszą brać udział w cyklicznych szkoleniach z bezpieczeństwa informacji.
- Grupa przeprowadza testy odporności na cyber zagrożenia, w których pracownicy uczestniczą.

## Odpowiedzialność za przestrzeganie Polityki

W tej części Polityki opisujemy odpowiedzialność za przestrzeganie jej:

- Każda spółka zależna musi wdrożyć zasady Polityki Bezpieczeństwa Informacji w swojej organizacji.
- Pracownicy muszą przestrzegać tych zasad i zgłaszać każde naruszenie.
- Pracownicy i kontrahenci muszą zachować w tajemnicy dane niepubliczne.

## Zgodność z przepisami prawa

Każda spółka zależna musi działać zgodnie z obowiązującymi przepisami prawa, regulacjami i dyrektywami, które dotyczą ochrony danych i bezpieczeństwa informacji.

## Konsekwencje naruszenia Polityki

W tej części Polityki opisujemy konsekwencje naruszenia Polityki:

- Złamanie zasad Polityki Bezpieczeństwa Informacji jest ciężkim naruszeniem obowiązków pracowniczych. Może prowadzić do zwolnienia dyscyplinarnego.
- Jeśli zasady naruszy kontrahent lub partner zewnętrzny, spółka może:
    - nałożyć kary umowne,
    - zakończyć współpracę natychmiastowo.
- Każde naruszenie Polityki musi być udokumentowane i zgłoszone jako incydent bezpieczeństwa.

## Przegląd i aktualizacja Polityki

W tej części Polityki opisujemy kto odpowiada za przegląd i aktualizację Polityki:

- Zarządy spółek zależnych i Chief Security Officer Grupy przeglądają Politykę przynajmniej raz w roku.
- Polityka jest aktualizowana, aby uwzględniać zmiany w prawie oraz nowe zagrożenia bezpieczeństwa informacji.