

## Polityka Bezpieczeństwa Powierzonych Danych - 00-00-53176-00

### §1. Wprowadzenie i definicje

1. Polityka Bezpieczeństwa Powierzonych Danych (dalej: **PBPD**) określa zasady postępowania w zakresie danych powierzonych do przetwarzania firmie Reynolds Medical Diagnostyka Kardiologiczna sp. z o.o. (dalej: **ADP**), w związku z realizacją zlecenia lub realizacją umowy, w tym w szczególności, w związku z zawartą umową powierzenia danych osobowych.
2. PBPD może zostać zmieniona w całości lub części przez ADP, w drodze indywidualnych zapisów, np. w wyniku zawarcia umowy powierzenia danych, umowy handlowej, umowy pomocy technicznej, poprzez indywidualne warunki oferty handlowej lub ekspertyzy technicznej. Zmiany wymagają formy pisemnej.
3. ADP zastrzega sobie możliwość wprowadzenia zmian do PBPD w dowolnym momencie, z tym że warunki te nie będą zmienione dla wcześniej rozpoczętych czynności i przyjętych do realizacji zleceń oraz umów.
4. **Informacje Poufne** - informacje stanowiące tajemnicę przedsiębiorstwa, w rozumieniu ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji które obejmują w szczególności: informacje techniczne, technologiczne, wszelkie dane o planach i specyfikacjach, informacje dotyczące oprogramowania, wynalazków lub jakichkolwiek rozwiązań, które mogą być chronione przez prawo autorskie, patentowe lub inne ustawy dotyczące własności intelektualnej, listy klientów, informacje dotyczące marketingu lub promocji dowolnego produktu, wszelkie plany działalności, a także informacje dotyczące handlowych lub organizacyjnych aspektów działalności oraz wszelkie informacje dotyczące lub zawarte we wprowadzonym i nie wprowadzonym na rynek oprogramowaniu; informacje nie stanowiące tajemnicy przedsiębiorstwa, jeżeli ze względu na okoliczności ujawnienia lub ich charakter powinny być traktowane jako poufne; informacje nie stanowiące tajemnicy przedsiębiorstwa, jeżeli ich przekazanie, ujawnienie lub wykorzystywanie mogłoby narazić na szkodę, zaszkodzić reputacji firmy lub któregokolwiek z jej klientów.
5. **Dane Osobowe** - dane w rozumieniu przepisów ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2002 r Nr 101, poz. 926 z późn. zm) - zwanej dalej również **UODO**.
6. **ADO** - administrator powierzanych danych osobowych, zgodnie z definicją UODO.
7. **ASI** - administrator systemu informatycznego
8. **Dane Kliniczne** - dane, które są zapisem sygnałów pacjenta lub wynikają z przetwarzania tego sygnału. Dane Kliniczne mogą zawierać Dane Osobowe.
9. **Dane Anonimowe** - Dane Kliniczne pozbawione Danych Osobowych.
10. **Próbka Danych** - jakiegokolwiek dane pobrane z systemu informatycznego w celu ich przetwarzania poza tym systemem.
11. **Zdalny Dostęp** - bezpośredni dostęp do systemu informatycznego realizowany poprzez publiczne łącza elektroniczne.

### §2. Poufność informacji

1. ADP podejmie odpowiednie środki bezpieczeństwa w stosunku do posiadanych Informacji Poufnych, co najmniej takie, jakie podejmuje w celu zabezpieczenia swoich własnych Informacji Poufnych.
2. Informacje Poufne przekazane w ramach realizacji umów i świadczeń, mogą być ujawniane wyłącznie na podstawie pisemnej zgody i wyłącznie w zakresie i w celu określonych przez taką zgodę. Zgoda nie może być dorozumiana z innych oświadczeń.
3. ADP może ujawniać Informacje Poufne tylko w sytuacjach, w których będzie do tego zobowiązany na podstawie bezwzględnie obowiązujących przepisów prawa.
4. ADP zobowiązuje się do zwrotu wszystkich otrzymanych w związku z wykonywaniem czynności i swoich obowiązków nośników, zawierających Informacje Poufne lub potwierdzi zniszczenie takich nośników, jeżeli ich zwrot nie jest możliwy.
5. ADP zobowiązuje się do nie ujawniania Informacji Poufnych przez okres 5 (pięciu) lat od daty zakończenia wykonywania świadczeń, w ramach których takie Informacje zostały przekazane.
6. Dane Kliniczne stanowią w ogólności Informacje Poufne, z wyłączeniem danych przekształconych do Danych Anonimowych.

### §3 Przetwarzanie danych osobowych

1. ADO wskazuje osobę fizyczną odpowiedzialną za Dane Osobowe powierzone ADP.
2. ADO określa właściwości rejestru lub zbioru powierzanych ADP Danych Osobowych.
3. ADP wskazuje i upoważnia osoby odpowiedzialne za przetwarzanie powierzonych Danych Osobowych ADO. Rejestr osób upoważnionych dostępny jest na każde uzasadnione wezwanie ADO.
4. Na żądanie ADO, osoby upoważnione zobowiązane są do przedstawienia upoważnień, z wyjątkiem sytuacji kiedy powierzone Dane Osobowe nie podlegają przetwarzaniu innemu niż związane przechowywaniem na nośnikach lub kiedy Zdalny Dostęp nie jest używany.
5. ADP zobowiązuje się przetwarzać Dane Osobowe wyłącznie w celu i w zakresie wcześniej uzgodnionym z ADO.
6. ADP zobowiązuje się do podjęcia przy przetwarzaniu powierzonych Danych Osobowych, środków zabezpieczających co najmniej w zakresie określonym w art. 36 do 39 UODO, w tym stosując się do właściwych w tym zakresie i aktualnych rozporządzeń.
7. ADP zobowiązuje się do informowania ADO o każdym podejrzeniu naruszenia bezpieczeństwa powierzonych Danych Osobowych oraz do współpracy w celu zapobieganiu naruszeniom, ograniczeniu ich skutków oraz naprawy powstałych z tego tytułu szkód.

8. ADP przetwarza powierzone Dane Osobowe bezpośrednio w systemie informatycznym lub przez Zdalny Dostęp.
9. ADP zastrzega sobie możliwość przetwarzania Próbkę Danych Osobowych w ramach przetwarzania powierzonych Danych Osobowych.
10. ADP zobowiązuje się do zniszczenia powierzonych Danych Osobowych w terminie do 5 (pięciu) dni roboczych od zaprzestania ich przetwarzania. W przypadku kiedy całkowite zniszczenie Danych Osobowych nie jest możliwe, np. w związku ze sposobem przechowywania i organizacji kopii zapasowych, ADP przekaze do ADO wszelkie informacje pozwalające na określenie miejsca przechowywania tych danych, sposobu ich zabezpieczenia i osób upoważnionych do dostępu do tych danych.

### **S3 Warunki realizacji przetwarzania danych**

11. ADO wskazuje podmiot lub osobę fizyczną wykonującą obowiązki ASI, właściwą dla powierzanego do przetwarzania rejestru lub zbioru danych.
12. ADP może odstąpić od przetwarzania danych w przypadku braku upoważnień dostępowych do systemu informatycznego, w którym znajdują się powierzone dane.
13. ADP wskazuje i upoważnia osoby posiadające dostęp do systemu informatycznego ADO. Rejestr osób upoważnionych dostępny jest na każde uzasadnione wezwanie ADO.
14. Przetwarzanie danych prowadzone jest w pierwszej kolejności poprzez Zdalny Dostęp.

Niniejsze PBPD obowiązują od dnia 1 czerwca 2016 r. do odwołania.

**[KONIEC] - 00-00-53176-00**