RODO w klubie
od 25 maja 2018 roku

Zmiany w przepisach o Ochronie Danych Osobowych

Co to jest RODO?

25 maja 2018 r. zacznie obowiązywać RODO czyli Rozporządzenie 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.

Czy RODO dotyczy klubów sportowych?

- **RODO obejmuje swoim zastosowaniem wszystkie podmioty prywatne i publiczne**, które przetwarzają dane (RODO Informator, Ministerstwo Cyfryzacji). W związku z tym wszystkie firmy, instytucje oraz organizacje **w tym kluby sportowe**, które zbierają i przetwarzają dane osobowe swoich członków, wolontariuszy, trenerów itp. (zarówno w formie papierowej jak i elektronicznej) muszą dostosować dotychczasowe procedury ochrony danych osobowych do nowych przepisów.

Przetwarzanie danych

- Wszystkie kluby powinny przestrzegać zasad przetwarzania danych osobowych zawartych w Artykule 5 RODO:
- Dane przetwarzane są zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.
- Dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
- Dane są prawidłowe i w razie potrzeby uaktualniane.
- Dane przechowywane są przez okres nie dłuższy, niż jest to niezbędne.
- Dane przetwarzane są w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych.

Co to są dane osobowe?

Dane osobowe to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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**, **kulturową lub społeczną tożsamość osoby fizyczne**j. (Art. 4 RODO)

Procedura wdrożenia RODO w klubie sportowym

RODO zakłada domyślną ochronę danych (Privacy by Default) oraz ochronę danych w fazie projektowania (Privacy by Design) (Art. 25 RODO). Administrator musi zdecydować jakie dane i w jakim celu przetwarza, a następnie tak określić zagrożenia oraz ryzyko wystąpienia naruszeń by odpowiednio zabezpieczyć przetwarzane dane osobowe. W celu wdrożenia zapisów RODO należy najpierw przeanalizować jak dotychczas wyglądało przetwarzanie i ochrona danych osobowych w Twoim klubie:

1. Jakie dane osobowe są przetwarzane w klubie, w czy są wśród nich dane szczególne (np. dotyczące zdrowia)?

2. Czy dane przetwarzane są legalnie , czyli np:

- za zgodą osób, których dotyczą;
- ich przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą; (czytaj dalej: Art. 6 RODO)

3. Jaki jest zakres i cel przetwarzania danych, tak by uniknąć przetwarzania danych nadmiarowych?
4. Jak przechowywane i zabezpieczone są dane w Twoim klubie?
5. Kiedy i w jaki sposób usuwane są dane osobowe?
6. Kto przetwarza dane osobowe i czy jest do tego upoważniony?
7. Czy dane przekazywane są innym podmiotom np. Związkowi Sportowemu, Urzędowi Gminy?
8. Czy przetwarzanie danych jest powierzane innym podmiotom np. usługi hostingowe, dane w chmurze?
9. Czy dane osobowe są przekazywane do państw trzecich (poza obszar UE)?
10. Czy osoby, których dane przetwarzamy zostały poinformowane o zakresie i celu przetwarzania ich danych osobowych oraz o prawach im przysługujących?

Znając odpowiedzi na powyższe pytania można przystąpić do wdrożenia przepisów RODO w klubie – Przeczytaj dalej !!!!

1. Zgoda na przetwarzanie danych osobowych

W przypadku klubu sportowego podstawą prawną do przetwarzania danych jest najczęściej zgoda osoby, której dane dotyczą, bądź w przypadku dziecka zgoda rodzica lub opiekuna prawnego. W związku z tym należy zweryfikować dotychczasową formę pobierania zgody i dostosować ją do nowych przepisów tak aby:

- Administrator (klub) był w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych;
- zapytanie o zgodę było przedstawione w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;
- osoba, której dane dotyczą, została poinformowana, że ma prawo w dowolnym momencie wycofać zgodę, a wycofanie zgody musi być równie łatwe co jej wyrażenie;
- mieć pewność, że zgoda została wyrażona dobrowolnie;

Podczas pozyskiwania zgody Administrator (klub) musi spełnić tzw. **obowiązek informacyjny**, dlatego należy z**weryfikować klauzulę informacyjną** podawaną każdorazowo, kiedy pozyskujemy dane osobowe i dostosować ją do nowych przepisów . Dokładne wytyczne dotyczące treści klauzuli informacyjnej można znaleźć w art. 13 RODO.

2. Rejestr czynności przetwarzania

Art. 30 RODO wprowadza obowiązek prowadzenia przez administratora danych ,,rejestru czynności przetwarzania", jeżeli:

- zatrudnia powyżej 250 osób;
- zatrudnia mniej niż 250 osób, ale przetwarzanie danych osobowych może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, przetwarzanie nie ma charakteru sporadycznego lub obejmuje szczególna kategorię danych osobowych, o których mowa w art. 9 RODO.

Mimo, że nie wszyscy administratorzy muszą prowadzić rejestr, to można zauważyć, że prowadzenie go ułatwia kontrolę nad przetwarzaniem danych osobowych. Wypełniając rejestr zgodnie z wytycznymi zawartymi w art. 30 RODO możemy określić cele przetwarzania, które muszą być podane osobom, których dane są przetwarzane, przeanalizować komu i jakie dane przekazujemy, w jaki sposób i jak długo przechowujemy dane, jak je zabezpieczamy i jakie jest ryzyko naruszenia praw lub wolności osób, których dane są przetwarzane.

Przykładowy Rejestr czynności przetwarzania można znaleźć na stronie www.giodo.gov.pl/pl/1520281/10449

3. Powierzanie przetwarzania danych

Jeżeli klub powierza przetwarzanie danych, których jest administratorem, innemu podmiotowi, to musi posiadać umowy powierzenia przetwarzania danych zgodnie z art. 28 i 29 RODO.

4. Upoważnienia do przetwarzania danych

Należy sprawdzić kto w klubie ma dostęp do danych i je przetwarza, a następnie wydać mu odpowiednie upoważnienie oraz prowadzić ewidencję takich upoważnień.

5. Prawa osób, których dane są przetwarzane

RODO kładzie szczególny nacisk na prawa przysługujące osobom, których dane są przetwarzane m.in.

- prawo do informacji dotyczących przetwarzania swoich danych;
- prawo do dostępu do swoich danych;
- prawo do sprostowania danych;
- prawo do usunięcia danych (,,bycia zapomnianym”);
- prawo do ograniczenia przetwarzania;
- prawo do przenoszenia danych;
- prawo do sprzeciwu;
- prawo do nie podlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu;

art. 13-22 RODO

Klub powinien być gotowy na wdrożenie odpowiednich procedur, które umożliwią realizację tych praw np. zastanowić się jak usuwać dane w razie, gdy osoba, której dane są przetwarzane będzie chciała skorzystać z prawa do ..bycia zapomnianym"? W odniesieniu do prawa do dostępu do swoich danych, osoba której dane dotyczą może wystąpić o wydanie kopii jej danych, które administrator przetwarza. Należy pamiętać, że nie można pobierać opłaty za wydanie pierwszej kopii, a sposób pobierania opłat za kolejne jest opisany w art. 15 RODO.

6. Naruszenia

Zgodnie z art.33 RODO administrator zobowiązany jest zgłosić naruszenie ochrony danych osobowych organowi nadzorczemu nie później niż 72 godziny po stwierdzeniu naruszenia. Treść zgłoszenia opisana jest w art.33 RODO. Administrator musi dokumentować wszystkie naruszenia ochrony danych osobowych np. kradzież danych (deklaracji członkowskich) lub włamanie do sieci komputerowej itp., w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze.
Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator musi jak najszybciej zawiadomić o naruszeniu osobę, której dane dotyczą (art. 34 RODO).

7. Polityka bezpieczeństwa danych osobowych

Zgodnie z ustawą z dnia 29 sierpnia 1997r. O ochronie danych osobowych, administrator był zobowiązany do przygotowania i wdrożenia polityki bezpieczeństwa danych osobowych oraz instrukcji zarządzania systemem informatycznym. Mimo, że RODO nie mówi wprost o obowiązku posiadania takiego dokumentu, administrator musi wykazać, jakie procedury ochrony danych wdrożył, jakie zabezpieczenia stosuje, jakie dane i w jakim celu przetwarza, jak monitoruje ryzyko wystąpienia naruszenia itp. dlatego w poradnikach RODO np. wydanych przez Ministerstwo Przedsiębiorczości i Technologii zaleca się dalsze stosowanie dokumentacji ochrony danych osobowych dostosowanej do przepisów zawartych w RODO, w szczególności dołączenie do niej rejestru czynności przetwarzania oraz analizy ryzyka (jeżeli są prowadzone).

Uwaga!

Powyższe informacje nie stanowią wytycznych dotyczących ochrony danych osobowych w klubach sportowych, mają na celu zwrócenie uwagi na zmiany w przepisach i zachęcić do zapoznania się z treścią rozporządzenia. Każdy klub, jako administrator danych osobowych, ponosi pełną odpowiedzialność za poprawne wdrożenie polityki bezpieczeństwa ochrony danych osobowych zgodnej z obowiązującym prawem.

Ważne linki

1. **Rozporządzenie 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)**

➢https://www.uodo.gov.pl/pl/131/224

2. **Ustawa z 10 maja 2018 o ochronie danych osobowych -** Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 30 sierpnia 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy o ochronie danych osobowych

➢https://www.uodo.gov.pl/pl/395/1192

Powyższe informacje zostały przygotowane w oparciu o stronę internetową http://szjudo.pl/rodo-w-klubie-od-25-maja-2018-roku/