

Sport ja isikuandmete kaitse üldmäärus (GDPR)

Mai 2018



25. mail 2018 jõustus uus EL-i isikuandmete kaitse üldmäärus (GDPR). GDPR-i kohaldamine muudab oluliselt seda, mil viisil on spordiorganisatsioonidel lubatud koguda ja töödelda oma liikmete (nt. sportlased, töötajad) ja kolmandate isikute isikuandmeid.

Kuna nimetatud uue paketi peamiseks eesmärgiks on parema kaitse tagamine EL-i kodanike isikuandmetele, mõjutavad nimetatud EL-i reeglid ka väljaspool EL-i asuvaid spordiorganisatsioone osas, milles nad koguvad ja töötlevad EL-i territooriumil asuvate inimeste isikuandmeid.

Käesoleva dokumendi eesmärgiks ei ole anda spordiorganisatsioonidele spetsiifilisi õiguslikke nõuandeid oma reeglite kooskõlla viimiseks uue õiguskorraga, vaid tuua välja võimalikud valdkonnad, kus EL-i GDPR-iga kooskõla tagamiseks võib osutuda vajalikuks täiendavate meetmete võtmine.

Sisukord

SISUKORD	1
I. ISIKUANDMETE KAITSE ÜLDMÄÄRUSE (GDPR) ÜLEVAADE.....	2
A. TAUST	2
B. EESMÄRGID	2
II. KONTROLL-LOEND SPORDIORGANISATSIOONIDELE	3
A. KAS UUS GDPR PUUDUTAB MINU ORGANISATSIOONI?.....	3
B. MILLISED MINU TEGEVUSTEST LOETAKSE ANDMETE TÖÖTLEMISEKS?	3
C. KAS MINU ORGANISATSIOONIS ON ISIKUANDMETE TÖÖTLEMISEGA SEOTUD VASTUTUSALAD HÄSTI PAIGAS? KAS MUL ON VAJA MÄÄRATA ISIK, KES VASTUTAB ISIKUANDMETE KAITSE ORGANISATSIOONISISESTE REEGLITE EEST?	4
D. KAS ORGANISATSIOONIS ON TAGATUD KÕIKIDE ISIKUANDMETE TÖÖTLEMISE ÕIGUSPÄRASUS?	4
E. MILLISEID PÄRINGUID VÕIB MINU ORGANISATSIOON ÜSIKISIKUTELT SAADA?	6
F. MIDA TULEKS SILMAS PIDADA LEPINGUTES, MIS ON SÕLMITUD KOLMANDATE ISIKUTEGA, KES TÖÖTLEVAID ISIKUANDMEID SINU EEST?	7
G. MILLEGA MA RISKIN, KUI EI KOHANDA OMA ISIKUANDMETE KAITSE REEGLEID? KAS MUL ON KOHUSTUS TEATADA ISIKUANDMETE RIKKUMISTEST?	7
III. ÜLEVAADE	8

I. Isikuandmete kaitse üldmääruse (GDPR) ülevaade

A. Taust

Isikuandmete kaitse on EL-i kodanike põhiõigus. See on sätestatud Euroopa Liidu põhiõiguste harta¹ artiklis 8, mille kohaselt on igal inimesel õigus oma isikuandmete kaitsele ning tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist.

Regulatsioon käsitleb isikuandmete töötlemist. Euroopa Komisjon esitas uue, 25. mail 2018 jõustuva isikuandmete kaitse paketi kavandi 2012. aastal ning see võeti vastu 2016. aasta aprillis pärast Euroopa Parlamendi (EP) ja nõukogu intensiivseid arutelusid. Määrus (EL) 2016/679 Euroopa Liidu (EL) uus isikuandmete kaitse üldmäärus (GDPR)², reguleerib EL-i isikuid puudutavate isikuandmete töötlemist üksikisikute, ettevõtete või organisatsioonide poolt.

B. Eesmärgid

GDPR on ette nähtud järgmiste eesmärkide täitmiseks:

- EL-i kodanike kaitse maailmamajanduse kontekstis, selle kohandamine interneti ja teiste uute tehnoloogiatega ning reeglite sätestamine, mis kehtiksid kõikide ettevõtete osas, olenemata sellest, kus need ettevõtted asuvad, kes töötlevad EL-i kodanike isikuandmeid.
- Anda üksikisikutele täielik kontroll oma isikuandmete üle, seades keskele kohale vabatahtliku nõusoleku ning andes kodanikele parema kontrolli selle üle, mida ja mis eesmärkidel nad jagavad.
- Tugevam kaitse isikuandmete rikkumiste vastu ning selle parem vastavus rikkumisele, kehtestades märkimisväärsed karistusi, mis hõlmavad võimalikke trahve summas kuni 4% aastasest globaalsest käibest või 20 miljonit eurot, olenevalt sellest, kumb nimetatud summadest on suurem.
- Uute ettevõtlusvõimaluste lubamine ühtsel turul harmoneeritud õigusraamistiku kaudu, aga ka isikuandmete rahvusvahelist ülekandmist puudutavate selgemate reeglite kaudu.

Määrus on kõikides liikmesriikides otsekohaldatav isegi kui mitmeid konkreetseid elemente on vaja defineerida liikmesriikide tasandil, kohandades selleks liikmesriikide seadusandlusi.

Kõik spordiorganisatsioonid, sh need, mis asuvad väljaspool EL-i, mis tegelevad EL kodanike isikuandmetega, peavad uut GDPR-i täitma.

¹ Euroopa Liidu põhiõiguste harta, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT>

² Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (EMPs kohaldatav tekst), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

II. Kontroll-loend spordiorganisatsioonidele

Alljärgnevatel punktides püüab EOC EL-i Esindus anda ülevaate mõningatest aspektidest, mida spordiorganisatsioonid peaksid arvesse võtma, et kontrollida oma isikuandmete kaitse reeglite kohaldamise vastavust ning ennast ette valmistada uueks õigussüsteemiks.

A. Kas uus GDPR puudutab minu organisatsiooni?

Uus GDPR puudutab kõiki spordiorganisatsioone nagu Rahvuslikud Olümpiakomiteed, rahvusvahelised, Euroopa ja riiklikud alaliidud, klubid või antidopinguagentuurid, kes koguvad, säilitavad ja töötlevad oma liikmete ja teiste isikute, sh EL-i territooriumil töötavate pealtvaatajate, sponsorite ja tarnijate isikuandmeid ning kindlustustega seotud isikuandmeid.

See kehtib sõltumata organisatsiooni asutamiskohast, sest kõik EL-i kodanike isikuandmeid koguvad ja töötlevad organisatsioonid on kohustatud neid reegleid täitma isegi kui nad asuvad väljaspool EL-i.

Väljaspool EL-i asuvad spordiorganisatsioonid (nt. EL-i välised Rahvuslikud Olümpiakomiteed, Euroopa ja rahvusvahelised föderatsioonid):

Kõik spordiorganisatsioonid, sealhulgas väljaspool EL-i asuvad organisatsioonid, kes tegelevad EL-i kodanike isikuandmetega, on kohustatud täitma uut GDPR-i. Teisisõnu, isikuandmete töötlemine langeb GDPR-i mõjusfääri niivõrd, kuivõrd selle objektiks on EL-i andmesubjektid nagu pealtvaatajad, ametnikud, töötajad või sportlased kes treenivad või võistlevad Euroopa Liidus.

Samuti sätestab GDPR-i artikkel 27 väljaspool EL-i asuvate üksuste, kellele ulatub GDPR-i territoriaalne kohaldamisala, kohustuse määrata kirjalikus vormis endale esindaja liidus. Esindajale tuleb anda volitus suhelda järelevalveasutustega ja andmesubjektidega kõigis isikuandmete töötlemisega seotud küsimustes, et tagada GDPR-i järgimine.

B. Millised minu tegevustest loetakse andmete töötlemiseks?

Isikuandmete töötlemine võib potentsiaalselt hõlmata mistahes tegevusi, mis toovad kaasa isikuandmete kogumise (nt. fännide või pealtvaatajate postiloendid (meililistid)), kasutamise (nt. sportlaste toitumine või tulemused) ja/või nende ülekandmise või saatmise (nt. tundlikud isikuandmed, tagamaks võistluste ausus).

Spordiorganisatsioonide kontekstis võivad sellisteks isikuandmeteks olla:

- spordiklubi liikmete isikuandmed;
- kolmandate isikute (nagu spordivõistluste pealtvaatajad, sponsorid, ...) isikuandmed;
- töötajate isikuandmed;
- e-kirja teel saadetavate infokirjade tellijate isikuandmed.

Tundlike isikuandmete nagu geneetilised andmed, terviseandmed või andmed seisukohtade ja uskumuste kohta, töötlemisele kohalduvad rangemad erinõuded (vaata allpool, küsimuse D juures).

C. Kas minu organisatsioonis on isikuandmete töötlemisega seotud vastutusalad hästi paigas? Kas mul on vaja määrata isik, kes vastutab isikuandmete kaitse organisatsioonisiseste reeglite eest?

Esimeseks sammuks oleks kaardistada oma praegused isikuandmete töötlemist puudutavad tegevused ning üle hinnata oma organisatsioonisisene menetlus. Eelkõige tuleb teil määratleda, millised isikuandmed on teie valduses ning mis eesmärgil ja mis õiguslikul alusel teil need on (vaata küsimus D). Kõiki teie klubi või alaliidu asjassepuutuvaid töötajaid tuleb informeerida vajadusest saavutada kooskõla uute isikuandmete kaitse reeglitega.

Tuleb koostada ülevaade oma isikuandmete töötlemist puudutavatest tegevustest (isikuandmete töötlemistoimingute kataloog), mis sisaldab informatsiooni selle kohta, milliseid isikuandmeid kogutakse, kellelt ja millisel eesmärgil ning kes selle eest vastutab. **Kõikide töödeldavate isikuandmete kirjelduste, töötlemise eesmärkide ja puudutatud isikute registri loomine on soovitatav kõikidele spordiorganisatsioonidele.**

Lisaks võib vajalikuks osutuda andmekaitse spetsialisti nimetamine, kes vastutab GDPR-i täitmise eest teie spordiorganisatsioonis – tingimused, millest tulenevalt see on vajalik, võivad sõltuda teie siseriiklikest regulatsioonidest. Andmekaitse spetsialist võib olla üks töötajatest, kes töötab ka muudel ametikohtadel, või väline teenusepakkuja. Teie organisatsioon peab tagama selle, et mitte ükski teine tööülesanne ei tekitaks andmekaitse spetsialistil huvide konflikti.

D. Kas organisatsioonis on tagatud kõikide isikuandmete töötlemise õiguspärasus?

Organisatsioonid peavad kontrollima ja tagama, et kõikide isikuandmete töötlemise õiguspärasus tugineb alljärgnevale õiguslikule alusele (artikkel 6).

- Andmesubjekt on andnud nõusoleku töödelda oma isikuandmeid. See peab olema konkreetne, teadlik, kehtiv ja ühemõtteline nõusolek, selge õigusega see tagasi võtta;
- See on „vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks“. Siiski kohalduv antud alus üksnes juhul, kui ülesanne täitmine on määratletud avalikes huvides olevaks liidu seadusandluse või vastutava töötleja osas kohalduva liikmesriigi seadusandluse kohaselt. Mõned liikmesriigid on siseriiklike seadustega määranud dopinguvastase võitluse avalikes huvides olevaks – seda puudutav hetkeolukord liikmesriikides oli Komisjoni mulluse uuringu³ teemaks.

³ Euroopa Komisjon: „Isikuandmete kaitset ja dopinguvastast võitlust puudutav uuring“, 19. oktoober 2017: <https://publications.europa.eu/en/publication-detail/-/publication/50083cbb-b544-11e7-837e-01aa75ed71a1/language-en/format-PDF/source-44694285>.

- Kui „isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral“. Korruptsioonivastane võitlus on üks näide õigustatud huvist sõltuvalt rahvuslikust seadusandlusest;
- Kui isikuandmete töötlemine on vajalik isiku osalusel sõlmitud lepingu täitmiseks (nt. liikmekaart või litsents, piletit ostev pealtvaataja).

Õiguslikule alusele peab tuginema ka üldiste isikuandmete töötlemine spordivõistlustel, sealhulgas andmed, mis puudutavad osalejaid, meeskondade või delegatsioonide koosseise, tulemusi või edetabeleid. **Sellega seoses soovitaksime teie organisatsioonil välja töötada nõusolekuvormi põhi, mille teie võistlustel osalevad sportlased või ametnikud saaksid allkirjastada ning mis puudutab isikuandmete erinevaid kasutusviise, mis võiksid teile tulevikus vajalikuks osutuda.**

Seni, kuni isikuandmeid kogutakse ja töödeldakse seaduspäraselt, ei esine nimetatud üldiste isikuandmete avaldamisel ja edastamisel põhimõtteliselt probleeme.

Isikuandmete töötlemise põhinormid:

- Seaduslikkus, õiglus ja läbipaistvus andmesubjektide osas;
- Eesmärgipiirangud: täpselt ja selgelt kindlaksmääratud ning õiguspärasel eesmärgidel ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus;
- Võimalikult vähesed isikuandmed: isikuandmed peaksid olema asjakohased, piisavad ja piirduma sellega, mis on nende eesmarke arvestades vajalikud.
- Õigsus: isikuandmed on õiged ja vajaduse korral ajakohastatud;
- Säilitamise piirang: isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse;
- Usaldusväarsus ja konfidentsiaalsus: isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid;
- Vastutus: vastutav töötleja vastutab käesolevate põhimõtete täitmise eest ja on võimeline seda tõendama.
- Kogutud isikuandmete turvalisuse ja konfidentsiaalsuse tagamine. Iga rikkumine peab kaasa tooma sanktsioonid (vaata küsimus G)

E. Milliseid päringuid võib minu organisatsioon eraisikutelt saada?

Juhul, kui te saate päringu sportlaselt, fännilt või ametnikult, on teil kohustus vastata sellele päringule 1 kuu jooksul ning sellelt eraisikult tasu võtmata.

Need õigused hõlmavad:

- Tutvumise õigus:

õigus tasuta tutvuda oma isikuandmetega. Juhul, kui te saate sellise päringu, olete te kohustatud:

- ütlema isikule, kas te töötlete tema isikuandmeid;
- teda töötlemisest teavitama (töötlemise eesmärk, asjaomaste isikuandmete kategooriad, andmete saajad jne.);
- esitama koopia töödeldavatest isikuandmetest.

- Taotlus isikuandmeid üle kanda: saada kõik isikuandmed üldkasutatavas ja masinloetavas vormis.
- Kustutamise taotlus (õigus olla unustatud).

Sellisel juhul on teie organisatsioon kohustatud kustutama kõik salvestatud isikuandmed, mis seda eraisikut puudutavad. Siiski esinevad erandid juhtudel, kus:

- isikuandmete töötlemine on vajalik sõna- ja teabevabaduse teostamiseks;
 - teil on kohustus säilitada isikuandmeid selleks, et täita juriidilist kohustust;
 - isikuandmete säilitamiseks esinevad muud avaliku huviga seotud põhjused nagu näiteks rahvatervis või teadus- või ajaloouringud
 - vajate isikuandmete säilitamist selleks, et koostada õigusnõudeid.
- Taotlus parandada ebaõigeid, ebatäpseid või ebatäielikke isikuandmeid.

Tundlike isikuandmete küsimus

„Tundlike isikuandmete”, mis hõlmavad andmeid rassilise või etnilise päritolu kohta, poliitiliste vaadete kohta, usuliste või filosoofiliste veendumuste kohta või ametiühingu liikmelisuse kohta ning geneetiliste või biomeetriliste andmete töötlemist füüsilise isiku unikaalse identifitseerimise eesmärgil, samuti tervisealaseid isikuandmeid või füüsilise isiku seksuaalelu või seksuaalset sättumust puudutavaid isikuandmeid, töötlemiseks eksisteerib üksnes piiratud hulk õiguslikke aluseid. See võib osutada oluliseks **antidopingu, võistlejate sugu puudutavate vaidluste, hormoonitasemete, spordis sugu määratlevate reeglite sõnastamise või treeningutel ja võistlustel tulemusi ja tervist puudutavate isikuandmete kogumise kontekstis.**

Võimalikud õiguslikud alused on nt:

- Selgesõnaline nõusolek;
- Oluline avalik huvi;
- Avalik huvi rahvatervise valdkonnas.

F. Mida tuleks silmas pidada lepingutes, mis on sõlmitud kolmandate isikutega, kes töötlevad isikuandmeid sinu eest?

GDPR paneb vastutavale isikuandmete töötlejale kõrge hoolsuskohustuse teenusepakkujate valikul, kes töötlevad ka isikuandmeid. Teenusepakkujatega - näiteks ürituste korraldajatega, avaliku sektori asutustega või eraõiguslike partneritega - sõlmitud lepingud peab sisaldama mitmesugust teavet (nt. töödeldavad isikuandmed ja töötlemise kestus) ning kohustusi (nt. abistamise kohustus juhul, kui leiab aset turvanõuete rikkumine, asjakohaste tehniliste ja korralduslike meetmete võtmise kohustus ning auditeerimisabi andmise kohustus). Tuleb samuti märkida, et lepinguid võib olla vaja kohandada ka teenustele, mis ei keskendu isikuandmete töötlemisele, kuid mille raames saab teenusepakkuja juurdepääsu isikuandmetele – näiteks IT ettevõtte, kelle tööülesandeks on arvutite ja serverite hooldustööd, mis võivad potentsiaalselt anda juurdepääsu isikuandmetele. Spordiorganisatsioonid peaksid seetõttu kaardistama oma koostöösuhted kolmandate isikutega, kes töötlevad neile kuuluvaid isikuandmeid või võivad potentsiaalselt saada juurdepääsu nendele isikuandmetele, ning kohandama neid lepinguid selliselt, et need vastaksid uutele isikuandmete kaitse reeglitele.

G. Millega ma riskin kui ma ei kohanda oma isikuandmete kaitse reegleid? Kas mul on kohustus teatada isikuandmete rikkumistest?

Trahvid võivad osutuda ränkadeks, kuna need võivad ulatuda 4 protsendini käibest (20 miljoni euro piires). (GDPR artiklid 82-84).

Lisaks sellele kehtib kõikidele spordiorganisatsioonidele üldine isikuandmete rikkumisest teavitamise kord. Kõikidest rikkumistest tuleb viivitusega teavitada järelevalveasutust, võimalusel mitte hiljem kui 72 tunni jooksul pärast rikkumisest teada saamist. On sätestatud nõuded, mida tuleb järelevalveasutusele teate saatmisel järgida (nt. kirjeldada isikuandmete rikkumise olemust, sealhulgas võimalusel kirjeldada puudutatud andmesubjektide kategooriaid ja ligikaudset arvu ning puudutatud isikuandmeid sisaldavate dokumentide kategooriaid ja ligikaudset arvu jne).

III. Ülevaade



Vaadake üle klubi / organisatsiooni privaatsuspõhimõtted ja isikuandmete õiglase töötlemise teated, tagamaks läbipaistvuse nõuete kohane täitmine.



Määrake, kes vastutab organisatsiooniselt isikuandmete töötlemise eest.



Viige läbi isikuandmete kaitse alane mõjuhindang mõistmaks, milliseid isikuandmed klubi või organisatsioon säilitab, kuidas ja miks seda tehakse ning määramaks kindlaks, mis on nimetatud isikuandmete kogumise ja säilitamise õiguspärane eesmärk. Looge isikuandmete töötlemistoimingute register.



Töötage välja nõusolekuavalduse vorm.



Analüüsige, kas ja millisel õiguslikul alusel töödeldakse teie organisatsioonis tundlikke isikuandmeid.



Vaadake üle isikuandmete kaitse meetmed, tagamaks isikuandmete turvalisus ja konfidentsiaalsus. Töötage välja kohased süsteemid isikuandmete kaitse rikkumiste puhuks.



Vajadusel nimetage andmekaitespetsialist.