Information om ClubRunner och GDPR

Den senaste tiden har det ställts en del frågor om ClubRunner uppfyller de regler om hantering av personuppgifter som finns i GDPR.

Det snabba svaret är: Ja, ClubRunner uppfyller kraven i GDPR. En Rotaryklubb i Sverige kan därför utan risk välja ClubRunner som verksamhetsstöd.

Men ClubRunner finns i Kanada, som ligger utanför EU? Får man verkligen föra över data till ett land utanför EU?

Ja, det går alldeles utmärkt, förutsatt att vissa kriterier är uppfyllda. I det här sammanhanget är det därför viktigt att ClubRunner finns just i Kanada. EU-kommissionen har nämligen granskat en massa länder och satt upp en lista över de som har en adekvat skyddsnivå i enlighet med GDPR. I denna lista finns Kanada med, vilket innebär att det är ok att föra över sin persondata dit.

Jag har sett att Kanada har en egen avdelning i den listan, det står något om ”kommersiellt” och ”om deras lagstiftning för skydd av personuppgifter i privat sektor är tillämplig på mottagarens personuppgiftsbehandling”.

Ja det är riktigt. Men ClubRunner är just en sådan kommersiell organisation som följer den kanadensiska dataskyddslagstiftningen PIPEDA, som i stora delar liknar GDPR. ClubRunner uppfyller därmed kraven på adekvat skyddsnivå enligt EU-kommissionen.

Ok då, men hur ser våra avtal med ClubRunner ut? Tar de på sig sitt ansvar i verkligheten också?

Ja. Mellan ClubRunner och respektive distrikt finns ett omfattande (18 sidor) avtal, ett s.k. Data Processing Addendum, som reglerar ClubRunners åtagande och ansvar. I detta avtal garanterar ClubRunner att följa europeisk lag rörande persondata, inklusive GDPR. Avtalet omfattar försäkringar om att hantera persondata i enlighet med GDPR, t.ex. att dokumentera alla åtgärder, att ha betryggande fysisk och datamässig säkerhet, att agera enligt GDPR vid ett dataintrång etc.

Att det är distriktet och inte klubben som har avtalet med ClubRunner beror på att affären med ClubRunner sker mellan distriktet och ClubRunner. Klubbarna är i sin tur medlemmar i distriktet, som tillhandahåller ClubRunner till dem. Klubbarnas användning av ClubRunner omfattas därmed av distriktets avtal.

Bra, men jag har hört att det finns ett särskilt avtal med en massa klausuler om datasäkerhet som kan skrivas med leverantörer utanför EU. Finns det ett sådant avtal med ClubRunner?

Du menar det ”standardklausulavtal” som EU-kommissionen har satt ihop för leverantörer som verkar i ett land som inte har adekvat dataskydd. Dessa ingår som en egen del i det ovan nämnda DPA-avtalet med ClubRunner. I detta garanterar ClubRunner även att ingen överföring sker till en ”sub-processor” i ett sådant tredje land utan ett skriftlig avtal om att denna ska följa GDPR och EU:s standardklausulavtal. Det innebär även att villkoren i EU-domstolens dom i det s.k. Schrems II-målet uppfylls av ClubRunner.

Just det, jag har också hört att vår medlemsdata även hanteras i USA, som EU inte anser vara ett land med adekvat skyddsnivå.

Ja, detta är dock en dubbel fråga, som både kan stämma och stämmer.

Om vi först går in på *”kan stämma”* så har ClubRunner möjlighet i enlighet med avtalet att använda underleverantörer (s.k. sub-processors) i andra länder. En sådan sub-processor är Microsofts globala Azurenätverk, som ClubRunner använder för molnlösningar och infrastruktur. Inom Azure körs själva programmet och databaserna. En annan är SendGrid, som är en av världens största hanterare av mejl och som ClubRunner använder för alla mejl som klubbarna skickar. Men det är fortfarande ClubRunner som är vår motpart och som har ansvaret gentemot oss. De gör en noggrann genomgång av dataskyddet hos sina underleverantörer och kräver i avtal att de ska uppfylla kraven som GDPR ställer (se ovan).

Tittar vi sen på *”stämmer”*, så stämmer det att medlemmarnas data även hanteras av Rotary International i USA och sannolikt Indien. *Detta är inget specifikt för ClubRunner utan gäller alla system som RI har godkänt.* ClubAdmin skickar t.ex. ständigt över medlemsdata från sina klubbar via ett privat hjälpsystem som heter Semda. Detta har gjorts i många år utan att de ansvariga i Sverige har ifrågasatt dataskyddet hos mottagaren. Denna överföring är dock en förutsättning för medlemskapet i Rotary och som sagt inte specifik för ClubRunner, vilket innebär att den ligger utanför ämnet för denna information.

Dock är det viktigt i sammanhanget att nämna att i klubbar som använder ClubRunner kan klubben ställa in vilka persondata utöver medlemmens namn som inte ska föras över till RI. Varje enskild medlem kan sen stärka skyddet ytterligare genom att stoppa även resterande uppgifter att föras över till RI. Varje enskild medlem kan även själv styra hur hen ska kunna sökas eller till och med stänga av sökning utanför klubben.

Så bra, det är ju nästan som Rätten om att bli glömd som finns i GDPR. Hur funkar det i ClubRunner?

Alldeles utmärkt, tackar som frågar. I ClubRunner kan man med ett enkelt knapptryck anonymisera en tidigare medlem. Anonymiseringen, som förvränger alla persondata till oigenkännlighet, gör det möjligt för klubben att ha kvar all statistik, t.ex. medlemsantal och närvaroprocent, trots att den tidigare medlemmens uppgifter inte längre är läsbara. ClubRunner uppfyller därmed Rätten att bli glömd i GDPR.

Informationen är sammanställd av Mats Håkanson, D2390, i juni 2021. Källor: Integritetsskyddsmyndigheten, the Government of Canada's Trade Commission, ClubRunner m.m.