

INTEGRITETSPOLICY FÖR RYHED IDROTT OCH REHAB AB

2018-05-25

Den 25 maj 2018 träder Dataskyddsförordningen i kraft vilket ställer fler krav på hur vi som företag hanterar personuppgifter i vårt arbete. För att möta förändringarna har **Ryhed Idrott och Rehab AB** arbetat fram följande dokument med de viktigaste förändringarna samt hur vi arbetar efter detta.

Innehållsförteckning

Dataskyddsförordningen	2
Information	3
Personuppgifter	3
Känsliga personuppgifter	3
Behandling Ryhed Idrott och Rehab AB s ansvar	3
Gallring	3
Rättelse	4
Radering	4
Registerutdrag	4
Säkerhet som standard	4
Rätt att behandla uppgifterna	4
Personuppgiftsincident	5
Insamlande av samtycke	6
Bilaga 1, Rutin för insamlande av samtycke	7
Bilaga 2, Rutin vid personuppgiftsincident	8

Dataskyddsförordningen

En ny EU-lag som ersätter personuppgiftslagen (PuL) för hur behandling av personuppgifter ska hanteras. Förordningen är likadan över hela EU vilket gör att det blir lättare att arbeta med personuppgifter mellan europeiska länder och den ställer dessutom högre säkerhets- och informationskrav än PuL på företag och organisationer som behandlar personuppgifter. Dataskyddsförordningen fokuserar på de patients rättigheter till sina uppgifter och lägger därför stor vikt vid dessa rättigheter och de medföljande skyldigheter som de företag som behandlar uppgifter har.

Information

Personuppgifter

En personuppgift är en uppgift som ensamt eller tillsammans med andra uppgifter kan användas av någon för att identifiera en nu levande fysisk person. Företagsuppgifter omfattas alltså inte.

Exempel på personuppgifter är: Personnummer, adress, e-post, telefonnummer, fastighetsbeteckning, medlemsnummer/kundnummer, registreringsnummer, IP-adress och fotografier på personer.

Alla uppgifter som ensamma eller tillsammans med andra uppgifter kan användas för att identifiera en fysisk person är en personuppgift. Det betyder att vi som företag som behandlar uppgifter måste säkra även uppgifter som ensamma inte kan identifiera en person men som i kombination med en eller flera andra uppgifter skulle kunna göra det.

Känsliga personuppgifter

Vissa kategorier av personuppgifter har bedömts vara så känsliga att de bara får behandlas om det finns direkt stöd i lag eller att patienten har gett sin uttryckliga tillåtelse. Om behandling är tillåten så måste dessutom extra stor hänsyn tas till säkerheten och patientens integritet.

Dessa uppgifter är: etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska eller biometriska uppgifter, hälsa eller sexuell läggning.

Det betyder att det är mycket viktigt vid registrering av nya noteringar, ändring av sparade noteringar eller uppgifter att kontrollera att de inte innehåller några känsliga personuppgifter som vi inte har laglig rätt att behandla. Endast om det verkligen är motiverat får en sådan uppgift sparas i journalsystemet. Om en kund skriver eller skickar in material som exempelvis innehåller hälsouppgifter och det inte är absolut nödvändigt för utförandet av vårt uppdrag ska inte sådana uppgifter sparas utan raderas efter att eventuella övriga uppgifter noterats i journalsystemet.

Behandling

När Ryhed Idrott och Rehab AB gör något med en personuppgift kallas det för att behandla uppgiften. När en uppgift behandlas måste det ske säkert och med skydd för integriteten för personuppgiften. En behandling är inte bara när vi tar upp information om en skada/sjukdom eller olyckshändelse och läser eller ändrar utan också att lagra uppgiften, när vi först registrerar uppgifterna i systemet eller att ta backup på databasen är att behandla uppgifter.

Ryhed Idrott och Rehab ABs ansvar

Ansvar för att behandlingen av uppgifterna sker korrekt ligger på hela Ryhed Idrott och Rehab AB med VD och styrelsen som ytterst ansvariga.

Gallring

Ryhed Idrott och Rehab AB får inte ha uppgifter i sina journalsystem som vi inte har behov av. "Bra att ha" uppgifter får inte sparas bara för att de är bra att ha. Det är därför viktigt att inte spara personuppgifter i mejl eller på andra platser än där det skall vara.

Rättelse

En person som är patient i något av Ryhed Idrott och Rehab ABs journalsystem har rätt att få sina uppgifter rättade om de är felaktiga. Det betyder att när en patient kontaktar Ryhed Idrott och Rehab AB och anger att uppgifterna inte är korrekta måste vi utreda om den information som patienten menar är felaktig faktiskt är det. Om det visar sig att informationen vi har registrerat är felaktig måste vi rätta den så snart som möjligt.

Vi måste alltid utreda om uppgifterna stämmer men behöver inte ändra om det visar sig att uppgifterna som den patient meddelar inte stämmer överens med vad vi vet eller kan se i offentliga register.

Radering

En person som är patient i något av Ryhed Idrott och Rehab ABs journalsystem har rätt att få sina uppgifter raderade om det inte längre finns behov av att ha uppgifterna kvar. Den patient måste då kontakta Ryhed Idrott och Rehab AB och meddela att den vill att vi tar bort all information om personen i våra journalsystem.

När en patient begär att bli raderad måste vi så snart som möjligt utreda om uppgifterna verkligen ska raderas. Kommer vi fram till att vi inte har behov av uppgifterna längre ska de raderas utan dröjsmål. Om utredningen visar att vi fortfarande har behov av uppgifterna då ska uppgifterna inte raderas.

Registerutdrag

En person som är patient i något av Ryhed Idrott och Rehab ABs journalsystem har rätt att få ett utdrag ur journalsystemet med allt som finns registrerat om personen. Journalutdraget är kostnadsfritt för den patient och lämnas antingen ut elektroniskt eller fysiskt, beroende på vad patienten önskar.

Säkerhet som standard

Dataskyddsförordningen kräver att journalsystem där personuppgifter behandlas sätter säkerhet främst, inte bara rent tekniskt utan även fysisk säkerhet i lokalerna samt rutiner för hur vi arbetar med personuppgifter i systemet.

Det innebär bland annat att vi har begränsningar i hur användare har rätt att använda systemen. Varje fysioterapeut kan använda "sitt" journalsystem men har inte rätt att använda sin kollegas.

Vi kommer fortfarande att ta emot e-post och skriva personuppgifter i journalsystem och träningsbok men de måste behandlas på samma säkra och lagliga sätt som all annan personuppgiftsbehandling.

Rätt att behandla uppgifterna

För att få behandla uppgifterna måste Ryhed Idrott och Rehab AB ha en rättslig grund som tillåter oss att behandla uppgifterna. De rättsliga grunderna är uppräknade i dataskyddsförordningen och inga andra än de som uttryckligen skrivits där är tillåtna.

De grunder som kan bli aktuella för Ryhed Idrott och Rehab AB är:

- Samtycke från den patient
- Behandlingen är nödvändig för att fullgöra ett avtal
- Det finns lagkrav eller myndighetsbeslut som kräver att uppgifterna behandlas
- Ryhed Idrott och Rehab AB har ett berättigat intresse att behandla uppgifterna

När det gäller behandling/rehab så har vi ett allmänt intresse att behandla uppgiften. Det betyder att det är i samhällets intresse att behandling/rehab utförs och fungerar som det ska.

Kontaktuppgifter för patienter som remitteras från landsting eller försäkringsbolag är också personuppgifter och måste behandlas som sådana. För behandling av sådana uppgifter har Ryhed Idrott och Rehab AB det som kallas berättigat intresse att behandla uppgifterna. Vid varje ny sådan behandling bedömer vi om vi har större intresse att behålla uppgifterna än vad patienten har av att vi tar bort den.

Personuppgiftsincident

En personuppgiftsincident är när personuppgifter oavsiktligt eller olagligt förstörs, förloras, ändras, sprids eller på annat sätt behandlas på ett sätt som kan skada eller kränka patienter.

Exempel på personuppgiftsincidenter är:

- Någon stjälar en dator där personuppgifter är sparade
- Någon tappar bort sin mobiltelefon som är kopplad till jobbmailen och innehåller sparade filer med personuppgifter
- En hacker tar sig in i databasen där alla gäldenärer finns sparade
- Flera aviseringar med olika mottagare hamnar i ett kuvert som skickas ut till remittent
- En anställd raderar felaktigt patientuppgifter
- Telefonerna havererar och ingen kan kontakta oss under ordinarie öppettider
- En eller flera datorer får sina hårddiskar krypterade av ett virus

Observera att listan inte är uttömmande och att fler situationer kan kvalificera som personuppgiftsincidenter.

Uppgifter behöver inte vara stulna eller ha kommit obehöriga tillhanda

En uppgift behöver inte vara stulen eller ha skickats till en obehörig för att det ska räknas som en incident. Det räcker exempelvis, som syns i listan, med att uppgifter förstörs trots att de skulle sparas för att det ska kvalificera som en incident.

Om det har hänt någonting med uppgifter om patient hos Ryhed Idrott och Rehab AB som det inte var tänkt att det skulle hända kan det vara en personuppgiftsincident. Därför kontrolleras den med ansvarige för dataskyddsfrågor om det uppstår en situation där personuppgifter utsatts för risk.

Vissa incidenter måste rapporteras till myndigheterna

Alla personuppgiftsincidenter måste registreras i Ryhed Idrott och Rehab ABs egna incidentregister men allvarligare incidenter måste också rapporteras vidare. Vid särskilt allvarliga incidenter måste dessutom de patienter som drabbats informeras.

En allvarlig personuppgiftsincident måste inom 72 timmar från det att Ryhed Idrott och Rehab AB blir medvetna om incidenten rapporteras till Integritetsskyddsmyndigheten (Datainspektionen). Rapporten är en standardiserad mall för rapportering av personuppgiftsincidenter som har tagits fram och finns hos ansvarig för dataskyddsfrågor hos Ryhed Idrott och Rehab AB

Om personuppgifter skickas fel, försvinner, ändras utan lov eller liknande

Kontaktas omedelbart Bengt Ryhed så fort felet upptäcks. Det är mycket viktigt att ansvarig personal får informationen så tidigt som möjligt då tidsfristen att rapportera en incident är kort och börjar löpa direkt när det upptäckts, oavsett vem som upptäcker det.

Insamlade av samtycke

I vissa situationer bör Ryhed idrott och rehab AB samla in samtycke från patient för att få behandla vissa uppgifter. Exempel är om försäkringsbolag eller arbetsgivare hör av sig och vill ha ut journalutdrag.

Rutin för insamlande av samtycke

2018-05-25, version 1

1. Verifiera personens identitet.

2. Informera om våra kontaktuppgifter:

- 2.1. Ryhed Idrott och Rehab AB behandlar dina personuppgifter i enlighet med dataskyddsförordningen. För kontakt med Ryhed Idrott och Rehab AB kan du antingen ringa 0278-139 90, maila på bengt@ryhed.com eller gå in på vår hemsida www.ryhed.com

3. Informera om villkoren för samtycket.

- 3.1. Dina uppgifter kommer att behandlas för att kunna journalföra, samt skriva träningsprogram, kontaktuppgifter, vi behandlar dina uppgifter med ditt samtycke.
- 3.2. Ryhed Idrott och Rehab AB samt våra personuppgiftebiträden, vilka exempelvis hjälper oss med utskrifter av fakturor, kan komma att ta del av dina uppgifter.
- 3.3. Uppgifterna kommer att sparas så länge de behövs för att uppfylla ändamålet eller till dess att ditt samtycke återkallas.
- 3.4. Du har som patient rätt att begära rättelse, radering samt begränsning av behandlingen av dina uppgifter, kontakta oss i sådant fall.
- 3.5. Du har närsomhelst rätt att återkalla ditt samtycke, kontakta oss då och meddela detta.

4. Informera om att patienten har rätt att klaga till Integritetsskyddsmyndigheten.

- 4.1. Om du inte är nöjd med informationen eller hur vi behandlat dina uppgifter enligt dataskyddsförordningen har du rätt att inge klagomål till Integritetsskyddsmyndigheten.

5. Notera att patienten samtyckt till personuppgiftsbehandling samt informerats om sina rättigheter enligt rutinen.

Bilaga 2, Rutin vid personuppgiftsincident

När du upptäcker en händelse som kan vara en personuppgiftsincident är det viktigt att du dokumenterar all information du har möjlighet i ärendet.

Ansvarig personal utreder sedan incidenten och vidtar därefter de nödvändiga åtgärder som behövs med bedömning av ärendets omständigheter och allvarlighet. Du kan behöva vara behjälplig under utredningen.

Ansvarig personal

Bengt Ryhed

Telefon: 070-670 94 67