GDPR

Finlands Svenska 4H

20.1.2026, Sebastian Gripenberg

Ansvar och begränsningar

1. Denna presentation utgör inte och är inte avsedd som rådgivning i något enskilt fall utan som en allmän introduktion till tematiken ur föreningars perspektiv utgående från offentliga källor och kan inte åberopas till stöd för att vidta eller avhålla sig från att vidta åtgärder. Framställningen är inte juridiskt uttömmande, heltäckande eller tillämpbar i alla fall. Hela förordningen, direktivet, den nationella lagstiftningen eller andra tillämpbara bestämmelser tas inte upp och tekniska lösningar beaktas inte. Åhöraren bör själv undersöka sitt fall på basis av en helhetsbedömning av alla relevanta faktorer och fatta beslut om vilka eventuella konsekvenser som i det egna fallet föranleds eller kan föranledas.
2. Trots att alla rimliga försök har gjorts för att garantera att alla citerade källor är korrekta tas inget ansvar för att all information är korrekt, aktuell, laglig eller fullständig. Presentationen är ett komplement till föreläsningen och är inte avsedd att vara ett fristående verk. Information som framställs som en tolkning bör inte accepteras som slutgiltig av åhöraren.
3. Materialet får internt användas fritt, men får inte publiceras på nätet eller spridas eller uppbevaras via sociala medier, molntjänster eller motsvarande kanaler som hör till informationssamhällets tjänster.

Översikt

Vad är GDPR?

Vad innehåller förordningen? (Tre viktiga helheter)

Lagliga grunder

Principer för behandlingen

Den registrerade rättigheter

Vad betyder det här i praktiken för vår organisation?

Allmänna synpunkter

- Synnerligen omfattande och komplicerad helhet – omöjligt att adekvat sammanfatta på den tid vi har.
  - 173 beaktandesatser (motiveringar, bakgrund) + 99 artiklar (paragrafer)
  - *Ca 100 sidor text, 55.000 ord + Dataskyddslagen (FI)*
- General Data Protection Regulation
  - Regulation = förordning (EU)
- Den högsta typen av lag inom EU-rätt. Gäller som så i medlemsstaterna.
- Trädde i kraft 22.5.2018. Väckte relativt stor uppmärksamhet för en EU-lag under upptakten – sedan har det varit tystare.

Allmänna synpunkter

- Komplicerad och delvis otydlig helhet
- Svepande, definitiva, men samtidigt allmänna, öppna formuleringar…
- Många tolkningar, mycket information i omlopp, delvis motstridigt – *mina tolkningar är välvilliga gentemot föreningar*
- Praxis utvecklas långsamt
  - ex. Iltalehti – vad är egentligen tillåtet, vad är förbjudet?
    - Förefaller uppenbart gå mot GDPR
  - Offentlighetsprincipen vs dataskydd i myndighetsverksamhet
    - Uppenbart inte avsikten

GDPR – vad ändrades?

- Största förändringen ur juridisk synpunkt: perspektivet ändrades:
  - tidigare: överensstämmelse, att följa reglerna (compliance)
  - NYTT: ansvarsskyldighet, skyldighet att kunna påvisa att man följer reglerna
- GDPR innehåller sanktionsmöjligheter som inte fanns i tidigare lagstiftning
- Betydligt mer detaljerad reglering samtidigt som vissa saker som fanns i tidigare lag inte tas upp (ex. ”registerbeskrivning” som begrepp finns inte med)
- Obs: GDPR gäller även på Åland, men Åland har en egen Datainspektion.

GDPR

- **Art. 2.1: Denna förordning ska tillämpas på sådan behandling av personuppgifter som**
  - **helt eller delvis företas på automatisk väg samt**
  - **på annan behandling av personuppgifter som ingår eller kommer att ingå i ett register.**

GDPR

- GDPR gäller alla organisationer som behandlar personuppgifter, både registerupprätthållare och de som behandlar personuppgifter, och s.g.s alla sammanhang där uppgifter behandlas, inte enbart medlemsregister / andra register
- Gäller alla – oberoende om det är frågan om en myndighet, ett företag eller en förening och oberoende hur omfattande behandlingen är, vilka uppgifter som behandlas eller vilken teknologi som används. GDPR är avsedd att vara vattentät – gäller allt och alla som har med personuppgifter att göra.
- Dessutom finns en nationell Dataskyddslag som kompletterar GDPR.

Omfattning

- *Beaktandesatser (4):*
  - Behandlingen av personuppgifter bör utformas så att den tjänar människor. **Rätten till skydd av personuppgifter är inte en absolut rättighet**; den måste förstås utifrån sin uppgift i samhället **och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen**. Denna förordning respekterar alla grundläggande rättigheter och iakttar de friheter och principer som erkänns i stadgan, såsom de fastställts i fördragen, särskilt skydd för privat- och familjeliv, bostad och kommunikationer, skydd av personuppgifter, tankefrihet, samvetsfrihet och religionsfrihet, yttrande- och informationsfrihet, näringsfrihet, rätten till ett effektivt rättsmedel och en opartisk domstol samt kulturell, religiös och språklig mångfald.
- **Alltså: det skydd och de rättigheter som GDPR erbjuder är inte absolut och heltäckande – skydd av personuppgifter kör inte *automatiskt* över alla andra rättigheter eller intressen, men det förefaller som om GDPR även har blivit en bekväm ursäkt.**

Undantag

Denna förordning ska inte tillämpas på behandling av personuppgifter som

a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,

b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget,

c) en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll,

d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

Undantag (beaktandesatserna)

- **<u>Gäller inte (bl.a.)</u>**
  - *Gäller inte avlidna personers personuppgifter (27)*
  - *Gäller personuppgifter – således inte ett medlemsregister där enbart organisationer är medlemmar, (men OBS en sådan förening sysslar också med **behandling av personuppgifter** i andra sammanhang) (14)*
  - *”Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt särskilda kriterier, bör inte omfattas av denna förordning” (15) (inte ordnade enligt särsk. krit. = de bildar inte ett register)*
  - *Uppgifter som har pseudonymiserats så att en fysisk person inte kan kännas igen eller kopplas till informationen omfattas inte. (26)*
- **Övriga undantag i GDPR eller Dataskyddslagen**
  - Undantag för bl.a. journalistiska ändamål och akademiskt, konstnärligt och litterärt skapande för att trygga yttrande- och informationsfrihet – men obs – vad som kan passera under dessa undantag är begränsat.

…kort parentes…

- Beaktandesats 15: ”[…] Akter eller grupper av akter samt omslag till dessa, som inte är ordnade enligt **särskilda kriterier**, bör inte omfattas av denna förordning. ”
  - *engelska: Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.*
- Kommentar: svårt att se praktiska situationer där akter inte är ordnade enligt **särskilda kriterier**. Exempelvis protokoll dateras.
  - Eventuellt anteckningar?
- Men trots det: icke-automatiserad behandling (dvs. manuell) som inte når eller är avsedd att nå tröskeln för att utgöra ett register faller utanför GDPR.
  - En hög av osorterade dokument utan digitala kopior i ett skåp omfattas inte av GDPR trots att de innehåller personuppgifter?

Undantag

- *Denna förordning är inte tillämplig på fysiska personers behandling av personuppgifter som ett led i verksamhet som är helt och hållet privat eller har samband med personens hushåll och därmed saknar koppling till yrkes- eller affärsmässig verksamhet. Privat verksamhet eller verksamhet som har samband med hushållet kan omfatta korrespondens och innehav av adresser, aktivitet i sociala nätverk och internetverksamhet i samband med sådan verksamhet. Denna förordning är dock tillämplig på personuppgiftsansvariga eller personuppgiftsbiträden som tillhandahåller utrustning för behandling av personuppgifter för sådan privat verksamhet eller hushållsverksamhet*. (Beaktandesats 18)
  - Kan gälla personuppgifter som behandlas för en fritidsaktivitet, hobby, semester eller nöje
  - Kan gälla kontaktuppgifter till vänner, info om deras bemärkelsedagar, hälsotillstånd o.dyl.
  - Kan gälla aktivitet i sociala medier
  - Ex. en övervakningskamera på ditt hus som även filmar en del av gatan är inte verksamhet av rent privat natur (EU-domstolen)
  - **Eventuell gråzon**: när är något ”rent privat” och när hör det till föreningen om t.ex. inga pengar rör sig via föreningen i samband med verksamheten?

GDPR – subjektiva synpunkter

- Idén är bra, tidigare lagstiftning var föråldrad – härstammade från medlet/slutet av 90-talet.
- Men:
  - Lagstiftningen är utvecklad med tanke på enorma multinationella företag, inte små, fattiga finlandssvenska föreningar – den gäller en alltför stor målgrupp, alla dras över samma kam – föregicks av kraftig lobbning, veterligen då trädde i kraft det mest ”lobbade” lagförslaget i EU:s historia.
    - Proportionalitet i resurser: Google vs Förening X rf
    - Absurt att en massa föreningar har varit tvungna att fundera om man kan ta bilder på sina tillställningar.
  - Texten är komplicerad, detaljerad men samtidigt svepande, övergripande, abstrakt och mycket kontextbunden. Alla svar på en fråga om GDPR inleds ”Det beror på…”. Litterärt ett mästerverk i sin genre.
  - Den största förändringen är ett perspektivskifte: tidigare regelefterlevnad, nu ansvarsskyldighet – skyldighet att kunna bevisa att man följer reglerna
  - Har något i praktiken ändrats på nätet? Urholkande av offentlighetsprincipen?
  - Vad har i praktiken ändrat inom föreningar: ytterligare en sak man inte hinner sköta ordentligt eller idel mönster av dataskydd??
  - Bra idé – hopplöst genomförande → bidrar i värsta fall till att minska tilltron till myndigheter och reglering i allmänhet. Har inte skapat tilltro till hur våra personuppgifter hanteras och har knappast främjat den digitala ekonomin. Nätet styrs av USA och Kina och EU är hopplöst efter.

GDPR - definitioner

- Art 4.1: **personuppgifter:** varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,
  - ***→ i praktiken vilken som helst uppgift som kan användas för att identifiera en fysisk person***

- *PuL: personuppgifter alla slags anteckningar som beskriver en fysisk person eller hans egenskaper eller levnadsförhållanden som kan hänföras till honom själv eller till hans familj eller någon som lever i gemensamt hushåll med honom,*

GDPR - definitioner

- Art 4.2: **behandling:** en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,
- *I praktiken s.g.s allt man kan hitta på att göra med en personuppgift*
- *PuL: behandling av personuppgifter insamling, registrering, organisering, användning, översändande, utlämnande, lagring, ändring, samkörning, blockering, utplåning och förstöring av personuppgifter samt andra åtgärder som vidtas i fråga om personuppgifterna,*

GDPR - definitioner

- Art 4.6: **register:** en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

- *PuL: personregister en datamängd som innehåller personuppgifter och som består av anteckningar som hör samman på grund av sitt användningsändamål, och som helt eller delvis behandlas med automatisk databehandling eller har ordnats som ett kartotek, en förteckning eller på ett annat motsvarande sätt så att information om en bestämd person kan erhållas med lätthet och utan oskäliga kostnader,*

- Särskilda kriterier innebär bl.a. att informationen är ordnad kronologiskt eller alfabetiskt eller i kategorier etc.

GDPR - definitioner

- Art 4.7: **personuppgiftsansvarig:** en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt,

- *PuL: registeransvarig en eller flera personer, sammanslutningar, inrättningar eller stiftelser för vilkas bruk ett personregister inrättas och vilka har rätt att förfoga över registret eller vilka enligt lag ålagts skyldighet att föra register,*

- **Dvs. föreningen är personuppgiftsansvarig – styrelsen bär ansvaret för att föreningen följer gällande lag. Kom ihåg: uppgifter kan delegeras i en förening, men inte ansvar. Om en uppgift delegeras måste vad som i praktiken händer följas upp och detta måste dokumenteras.**

GDPR

- Tanken är att fysiska personer ska ha en omfattande rätt till alla uppgifter som de kan identifieras med hjälp av – *men den kör inte automatiskt över alla andra rättigheter*.

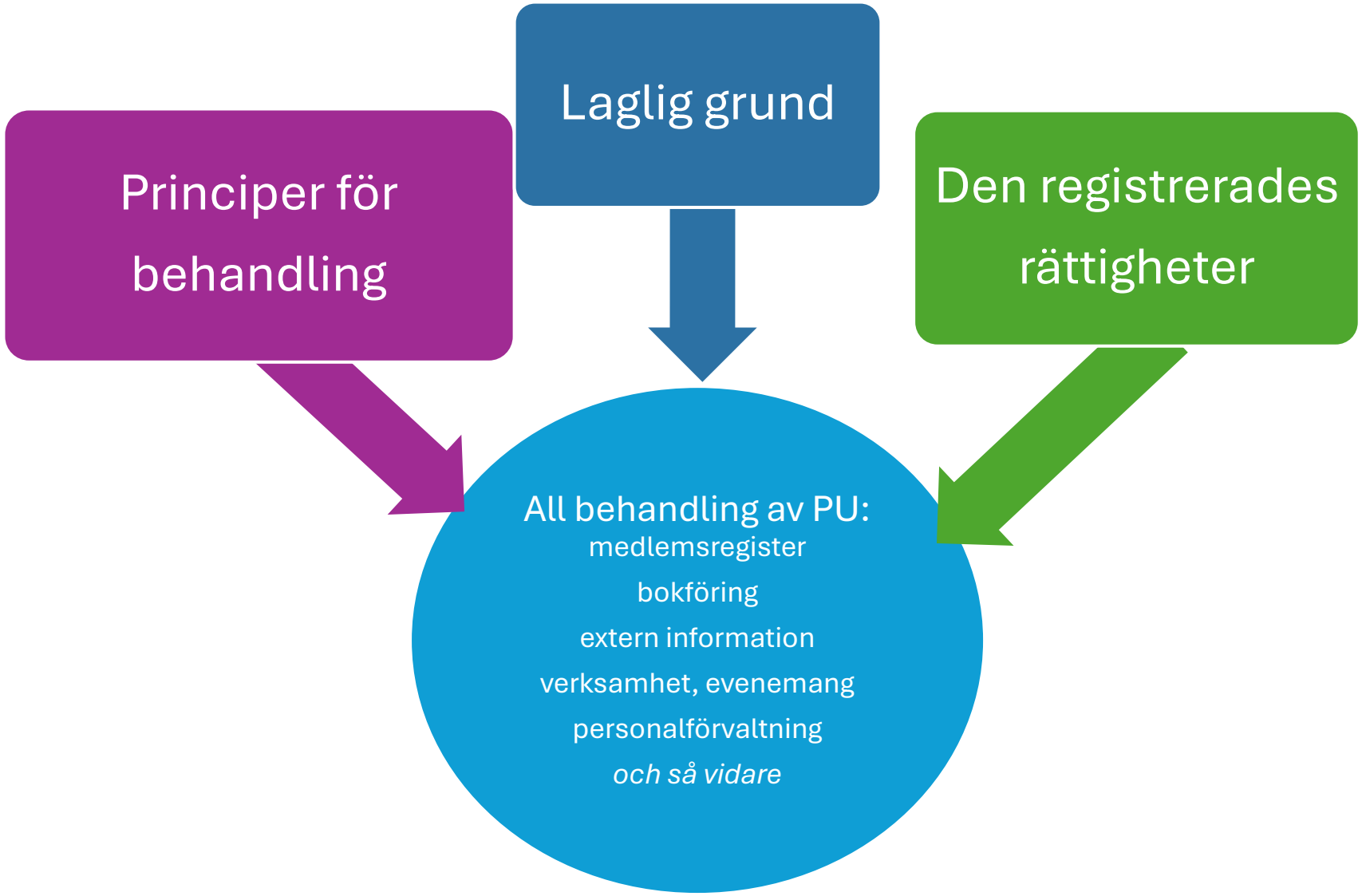
- När personuppgifter samlas in och används ska den registrerade ha omfattande rättigheter i förhållande till den som samlar in och använder dem.

- OBS: **det är inte förbjudet att behandla personuppgifter** – behandlingen måste helt enkelt ske enligt vissa regler

Ur föreningens perspektiv

- Tre centrala helheter som måste beaktas:
  1. Laglig grund
     - För att kunna behandla personuppgifter måste organisationen ha en laglig grund för det
  2. Principer för behandlingen
     - Om en laglig grund finns måste behandlingen ske enligt vissa principer
  3. Den registrerades rättigheter
     - Genom hela behandlingen måste organisationen kunna garantera vissa rättigheter som varje person har

  - Ansvarsskyldigheten innebär alltså att den personuppgiftsansvariga måste ha koll på dessa tre helheter och kunna påvisa att man har koll på dem.


Principer för behandling
Laglig grund
Den registrerades rättigheter
All behandling av PU:
medlemsregister
bokföring
extern information
verksamhet, evenemang
personalförvaltning
och så vidare

Gdpr – laglig grund

ART 6.1: Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

a) Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.

b) Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

c) Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

d) Behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person.

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

f) **Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen**, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Led f i första stycket ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

Laglig grund för föreningar

- Samtycke (6.1.a)
- Rättslig förpliktelse (6.1.c)
- Berättigat intresse (6.1.f)

- Övriga i princip möjliga men mer sällsynta i praktiken.

Laglig grund – rättsliga förpliktelser

- Föreningslagen: 11§1mom: ”Styrelsen skall föra en **förteckning över föreningens medlemmar**. I förteckningen skall införas varje medlems fullständiga namn och hemort.”
  - ➔ föreningar har en lagstadgad skyldighet att upprätthålla ett register över sina medlemmar och har med stöd att föreningsfriheten rätt att registrera sådana uppgifter som är nödvändiga och logiska med tanke på verksamheten
  - OBS: Dataombudsmannen skriver att föreningslagen 11§1mom endast gäller de uppgifter som däri nämns. För övriga uppgifter anges att samtycke behövs – men är det rimligt? De övriga uppgifterna bör i de flesta föreningar med sedvanlig verksamhet **kunna utgöra berättigat intresse** (sedvanliga kontaktuppgifter)
- **bokföring** är en rättslig förpliktelse och kan innehålla många personuppgifter, ex. inbetalda medlemsavgifter, utbetalade arvoden, löner, kostnadsersättningar, reseräkningar, deltagarförteckningar etc.
- **Anställda** – arbetslagstiftning, arbetsavtalslagen
- föreningar är skyldiga att göra vissa **anmälningar till myndigheter**, PRS, skatteverket, banker etc.
- föreningar kan ha rättsliga förpliktelser ex. i samband med **redovisning av offentliga understöd**
  - (…och ett berättigat intresse att **redovisa privata understöd**.)
- ”Rättsliga förpliktelser” kan inte åberopas hur som helst. Behandlingen måste uttryckligen förutsättas i en lag att behandlingen sker och den personuppgiftsansvariga skall inte ha något val**.**

- **Behandling som grundar sig på 6.1.c eller 6.1.f kräver inte ett skilt samtycke av den registrerade personen**

Laglig grund

- Observera också **beaktandesats 48**:
- Personuppgiftsansvariga som ingår i en koncern eller **institutioner som är underställda ett centralt organ kan ha ett berättigat intresse att överföra personuppgifter inom koncernen för interna administrativa ändamål**, bland annat för behandling av kunders eller anställdas personuppgifter. De allmänna principerna för överföring av personuppgifter, inom en koncern, till företag i tredjeland påverkas inte.

Laglig grund – berättigat intresse

”Henkilötietojen käsittely voi toisinaan olla perusteltua rekisterinpitäjän tai kolmannen osapuolen oikeutetun edun takia. Oikeutettu etu käsittelyperusteena edellyttää, että rekisteröidyn edut ja oikeudet huomioidaan erityisen tarkkaan.

Oikeutettu etu voi olla olemassa *esimerkiksi* silloin, kun rekisteröidyn ja rekisterinpitäjän välillä on jokin merkityksellinen suhde. Se tarkoittaa, että rekisteröity on ***esimerkiksi*** rekisterinpitäjän asiakas tai alainen.

Se, milloin etu voidaan katsoa oikeutetuksi, saadaan selville niin kutsutulla **tasapainotestillä**. *Siinä rekisterinpitäjän tai kolmannen osapuolen intressiä punnitaan rekisteröidyn intressejä ja perusoikeuksia vasten*.

Tietosuoja-asetuksen myötä oikeutetun edun perusteella voidaan tehdä myös muita käsittelytoimenpiteitä, jos se on tasapainotestin perusteella mahdollista.”

- Källa: www.tietosuoja.fi, 9.4.2018

Laglig grund – berättigat intresse

- Behandlingen med stöd av ett berättigat intresse måste vara nödvändig.
  - Om resultatet kunde åstadkommas på något annat sätt bör det gå före
- Den registrerades intressen och rättigheter måste vägas mot den personuppgiftsansvariges berättigade intresse – man måste kunna demonstrera hur man har resonerat då man hävdar ett berättigat intresse.
- Ex.
  - mingelbilder, förutsatt att saken nämns i inbjudan?
    - Praxis har blivit samtycke i samband med anmälan.
  - Kontaktuppgifter för information?

Laglig grund – samtycke

- Art 7:
  - **1.Om behandlingen grundar sig på samtycke, ska den personuppgiftsansvarige kunna visa att den registrerade har samtyckt till behandling av sina personuppgifter.**
  - 2.Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, ska begäran om samtycke läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Om en del av förklaringen innebär en överträdelse av denna förordning, ska denna del inte vara bindande.
  - **3.De registrerade ska ha rätt att när som helst återkalla sitt samtycke.** Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycke, innan detta återkallas. Innan samtycke lämnas ska den registrerade informeras om detta. Det ska vara lika lätt att återkalla som att ge sitt samtycke.
  - 4.Vid bedömning av huruvida samtycke är frivilligt ska största hänsyn bland annat tas till huruvida genomförandet av ett avtal, inbegripet tillhandahållandet av en tjänst, har gjorts beroende av samtycke till sådan behandling av personuppgifter som inte är nödvändig för genomförandet av det avtalet.

Laglig grund – samtycke

- GDPR understryker betydelsen av samtycke. **Samtycke är s.a.s. huvudregeln**.
- Föreningar måste beakta detta, kanske inte i samband med medlemsregistret, men eventuellt i andra sammanhang där personuppgifter samlas in.
- Personuppgifter samlas in i många andra sammanhang som en del av verksamheten: anmälningar, deltagarförteckningar, personuppgifter på personer som inte är medlemmar etc.
  - Den här ”diffusa” insamlingen är mer problematisk för föreningen – den bygger inte på en lagstadgad skyldighet utan på samtycke eller berättigat intresse => lönar sig för föreningar att så långt som möjligt försöka hålla behandlingen inom **6.1.c eller 6.1.f**
  - **GDPR visar hur viktigt det är att ha medlemsregistret uppdaterat, att de personer man har i sin målgrupp verkligen är medlemmar och att så mycket som möjligt av den här behandlingen utgår från medlemsregistret**
  - Personuppgifter för personer som inte är medlemmar är svårare
  - Samtycke är ett tveeggat svärd: samtycke möjliggör en omfattande behandling (allt det man samtycker till), men samtycke kan när som helst återtas → besvärligt för föreningen att hantera.

Barn

- Art 8.1: Vid erbjudande av **informationssamhällets tjänster** direkt till ett barn, ska vid tillämpningen av artikel 6.1 a [=samtycke] behandling av personuppgifter som rör ett barn vara tillåten om barnet är minst 16 år. Om barnet är under 16 år ska sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet.
  - Fi Dataskyddslag: 13 år
  - OBS – medlemskap i en förening är inte ”informationssamhällets tjänster”
  - Barn har rätt att vara medlem i en förening – men tillstånd av föräldrar om under 13 år för att behandla personuppgifter – på motsv. sätt info t.ex. om dieter o. sådant för anmälningar till läger etc.
  - Bilder på barn – tillstånd av föräldrar i förväg (samtycke)

  - OBS! Beaktandesats (38): *Samtycke från den person som har föräldraansvar över barnet bör inte krävas för förebyggande eller rådgivande tjänster som erbjuds direkt till barn*.

GDPR – känsliga/förbjudna uppgifter

- Art 9.1: 1.Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning **ska vara förbjuden**.

- Jmfr PuL: Förbud mot behandling av känsliga uppgifter
  - Behandling av känsliga personuppgifter är förbjuden. Med känsliga uppgifter avses personuppgifter som beskriver eller vilkas syfte är att beskriva
  - 1) ras eller etniskt ursprung,
  - 2) någons samhälleliga eller politiska uppfattning eller religiösa övertygelse eller medlemskap i ett fackförbund,
  - 3) en brottslig gärning eller ett straff eller någon annan påföljd för ett brott,
  - 4) någons hälsotillstånd, sjukdom eller handikapp eller vårdåtgärder eller därmed jämförbara åtgärder som gäller honom,
  - 5) någons sexuella inriktning eller beteende, eller
  - 6) någons behov av socialvård eller de socialvårdstjänster, stödåtgärder och andra förmåner inom socialvården som någon erhållit.

GDPR – känsliga/förbjudna uppgifter

- Många undantag: t.ex.
  - den registrerade har uttryckligen lämnat sitt samtycke (Art 9.2.a)
  - **Behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen enbart rör sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och personuppgifterna inte lämnas ut utanför det organet utan den registrerades samtycke. (Art 9.2.d)**
    - **Men:** Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder enligt artikel 6.1 får endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet. (Art 10)
  - OBS! Beaktandesats (51): Behandling av foton bör inte systematiskt anses utgöra behandling av känsliga uppgifter. Foton är biometriska uppgifter endast när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person.

…kort parentes…

- Artikel 9.2.d är intressant eftersom den innehåller ett mycket omfattande undantag.
- Den tillåter behandling av uppgifter som i övrigt är förbjudna på mer omfattande grunder än artikel 6.
- Ifall:
  - Gäller berättigad verksamhet hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte
  - Lämpliga skyddsåtgärder används och
  - Uppgifterna inte lämnas ut utan samtycke
- Så får förbjudna uppgifter behandlas som
  - rör sådana organs medlemmar eller tidigare medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta
- *Är det alltså lättare att behandla ”förbjudna uppgifter” än ”normala uppgifter” (uppgifter som inte förbjuds enl. art.9.1)?*
- Å andra sidan tyvärr inte klart att varje **ideellt syfte** utgör ett ”**politiskt, filosofiskt, religiöst eller fackligt syfte**”
  - Antyder ett syfte som berör världsåskådning. Lusläs föreningens syfte…

Möjliga lagliga grunder i några typiska fall

- Medlemsregister: rättsliga förpliktelser och berättigat intresse eller rättsliga förpliktelser och samtycke (föreningslagen)
- Anställda: rättsliga förpliktelser och berättigat intresse
- Anmälningar
  - medlemmar: en del av medlemsregisterbehandlingen
  - Icke-medlemmar: samtycke eller berättigat intresse
  - Dieter etc i samband med anmälningar: undantag i 9.2.d ?
- Deltagarförteckningar: t.ex. kan i vissa fall höra till bokföring i s.f. -> rättsliga förpliktelser – annars samtycke eller berättigat intresse
- Bilder från tillställningar: berättigat intresse (meddela i förväg) eller samtycke
- Kontaktuppgifter till icke-medlemmar (för info): berättigat intresse (motsv. direkt marknadsföring) – samtycke besvärligt?
- Föreningens tidning: undantag för journalistiska ändamål? Eventuellt i vissa fall.
- En historik: undantag för litterärt skapande?
- Protokoll: berättigat intresse, årsmötesprotokoll: rättslig förpliktelse

GDPR – principer för behandling

- Art 5: 1. Vid behandling av personuppgifter ska följande gälla:
  - a) Uppgifterna ska behandlas på ett **lagligt, korrekt och öppet sätt i förhållande till den registrerade** (*laglighet, korrekthet och öppenhet*).
  - b) De ska samlas in för **särskilda, uttryckligt angivna och berättigade ändamå**l och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (*ändamålsbegränsning*).
  - c) De ska vara **adekvata, relevanta och inte för omfattande** i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).
  - d) De ska vara **korrekta och om nödvändigt uppdaterade**. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (*korrekthet*).

GDPR – principer för behandling

- e) De får inte förvaras i en form som **möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas**. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (*lagringsminimering*).
- f) De ska behandlas på ett sätt som **säkerställer lämplig säkerhe**t för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).

- **2.Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (*ansvarsskyldighet*).**

den registrerades rättigheter

- Förordningen tar upp och preciserar många rättigheter som den registrerade har i förhållande till den som upprätthåller registret.
- ➔ Det gäller även föreningsmedlemmar i förhållande till föreningens medlemsregister.

den registrerades rättigheter - översikt

- Art 12: hur den personuppgiftsansvariga skall agera
- Art 13: Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade
- Art 14: motsvarande om personuppgifterna samlas in indirekt
- Art 15: rätt till tillgång
- Art 16: rätt till rättelse
- Art 17: rätt till radering
- Art 18: rätt till begränsning av behandling
- Art 19: anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling
- Art 20: rätt till dataportabilitet (torde inte påverka föreningar?)
- Art 21: rätt att göra invändningar
- Art 22: Automatiserat individuellt beslutsfattande, inbegripet profilering (torde inte påverka föreningar?)

GDPR – den registrerades rättigheter

- Art 12.1: Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla all information som avses i artiklarna 13 och 14 och all kommunikation enligt artiklarna 15–22 och 34 vilken avser behandling i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.
  - 13 = Information som ska tillhandahållas om pers.uppg. samlas in från den registrerade
  - 14 = Information som ska tillhandahållas om pers.uppg. inte har erhållits från den registrerade (tas inte upp här)
  - 15-22 = specifika rättigheter som tillkommer den registrerade
  - 34 = information till den registrerade om en personuppgiftsincident

GDPR – den registrerades rättigheter

- D.v.s. ➔ All kommunikation med den registrerade skall ske i skriftlig form, om inte den registrerade begär informationen muntligt, men också i så fall enbart om föreningen är säker på den registrerades identitet. Kommunikationen ska vara koncis, klar och tydlig, begriplig och i lätt tillgänglig form, med användning av klart och tydligt språk.
  - Muntlig information endast vid personligt besök och endast om man känner igen medlemmen.

GDPR – den registrerades rättigheter

- Art 12.2: Den personuppgiftsansvarige ska **underlätta utövandet av den registrerades rättigheter** i enlighet med artiklarna 15–22. I de fall som avses i artikel 11.2 får den personuppgiftsansvarige inte vägra att tillmötesgå den registrerades begäran om att utöva sina rättigheter enligt artiklarna 15–22, om inte den personuppgiftsansvarige visar att han eller hon inte är i stånd att identifiera den registrerade.
- Art 12.3: Den personuppgiftsansvarige ska **på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits enligt artiklarna 15–22**. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden. Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen. Om den registrerade lämnar begäran i elektronisk form, ska informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat.

GDPR – den registrerades rättigheter

- Art 12.4: Om den personuppgiftsansvarige inte vidtar åtgärder på den registrerades begäran, ska den personuppgiftsansvarige utan dröjsmål och senast en månad efter att ha mottagit begäran informera den registrerade om orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till en tillsynsmyndighet och begära rättslig prövning.
- D.v.s → **Om man inte gör något är man ändå skyldig att meddela det. Skall vara omöjligt att inte reagera.**

GDPR – den registrerades rättigheter

- Art 12.5: Information som tillhandahållits enligt artiklarna 13 och 14, all kommunikation och samtliga åtgärder som vidtas enligt artiklarna 15–22 och 34 ska tillhandahållas **kostnadsfritt.** Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige antingen a) ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller b) vägra att tillmötesgå begäran. Det åligger den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller orimlig.

GDPR – den registrerades rättigheter

- (Art 12.6) → Om det finns **rimliga skäl att betvivla identiteten** hos den person som lämnar in en begäran, får föreningen begära att ytterligare information som är nödvändig för att bekräfta den registrerades identitet, tillhandahålls.
  - T.ex. → om en medlem skickar en begäran från en annan e-postadress än den som föreningen har i sitt medlemsregister?
  - Om föreningen inte har e-postadresser i sitt medlemsregister? > ev. så: Informationen postas till den adress som finns i registret.
  - Om föreningen endast har namn och hemort i registret?

GDPR – den registrerades rättigheter

- Art 13 Information som ska tillhandahållas om personuppgifterna samlas in från den registrerade
- (1) Om personuppgifter som rör en registrerad person samlas in från den registrerade, ska den personuppgiftsansvarige, **när personuppgifterna erhålls**, till den registrerade lämna information om följande:
  - a) Identitet och kontaktuppgifter för den personuppgiftsansvarige och i tillämpliga fall för dennes företrädare.
  - b) Kontaktuppgifter för dataskyddsombudet, i tillämpliga fall.
  - c) Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen.
  - d) Om behandlingen är baserad på artikel 6.1 f, den personuppgiftsansvariges eller en tredje parts berättigade intressen.
  - e) Mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna, i förekommande fall.
  - f) I tillämpliga fall att den personuppgiftsansvarige avser att överföra personuppgifter till ett tredjeland eller en internationell organisation och huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, när det gäller de överföringar som avses i artikel 46, 47 eller artikel 49.1 andra stycket, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

GDPR – den registrerades rättigheter

- (2) Utöver den information som avses i punkt 1 ska den personuppgiftsansvarige vid insamlingen av personuppgifterna lämna den registrerade följande ytterligare information, vilken krävs för att säkerställa rättvis och transparent behandling:
  - a) Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
  - b) Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.
  - c) Om behandlingen grundar sig på artikel 6.1 a eller artikel 9.2 a, att det föreligger en rätt att när som helst återkalla sitt samtycke, utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
  - d) Rätten att inge klagomål till en tillsynsmyndighet.
  - e) Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav eller ett krav som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att sådana uppgifter inte lämnas.
  - f) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

GDPR – den registrerades rättigheter

- (3) Om den personuppgiftsansvarige avser att ytterligare behandla personuppgifterna för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om detta andra syfte samt ytterligare relevant information enligt punkt 2.
- (4) Punkterna 1, 2 och 3 ska inte tillämpas om och i den mån den registrerade redan förfogar över informationen.

- D.v.s → Art 13 motsvarar närmast den **registerbeskrivning** som en registeransvarig tidigare måste ha, men är betydligt mer detaljerad och ställer högre krav på att den registrerade ska få den här informationen. (Nu räcker det att den är ”allmänt tillgänglig”)

GDPR – den registrerades rättigheter

- Art 14 – om man har fått personuppgifterna av någon annan än den person det gäller…
  - Motsvarande som artikel 13

GDPR – den registrerades rättigheter

- Art 15 – Den registrerades rätt till tillgång
- 1.Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och följande information:
  - **a) Ändamålen med behandlingen.**
  - **b) De kategorier av personuppgifter som behandlingen gäller.**
  - **c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.**
  - **d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.**
  - **e) Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling.**
  - **f) Rätten att inge klagomål till en tillsynsmyndighet.**
  - g) Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.
  - h) Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.
- 3.Den personuppgiftsansvarige ska förse den registrerade **med en kopia av de personuppgifter** som är under behandling. För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift på grundval av de administrativa kostnaderna. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.

GDPR – den registrerades rättigheter

- Art 16: **Rätt till rättelse**
  - Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålet med behandlingen, ska den registrerade ha rätt att komplettera ofullständiga personuppgifter, bland annat genom att tillhandahålla ett kompletterande utlåtande.

GDPR – den registrerades rättigheter

- Art 17: **Rätt till radering (”rätten att bli bortglömd”)**
  - Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få sina personuppgifter raderade och den personuppgiftsansvarige ska vara skyldig att utan onödigt dröjsmål radera personuppgifter om något av följande gäller:
    - **a) Personuppgifterna är inte längre nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats.**
    - b) Den registrerade återkallar det samtycke på vilket behandlingen grundar sig enligt artikel 6.1 a eller artikel 9.2 a och det finns inte någon annan rättslig grund för behandlingen.
    - c) Den registrerade invänder mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre, eller den registrerade invänder mot behandlingen i enlighet med artikel 21.2.
    - d) Personuppgifterna har behandlats på olagligt sätt.
    - e) Personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av.
    - f) Personuppgifterna har samlats in i samband med erbjudande av informationssamhällets tjänster, i de fall som avses i artikel 8.1.

- D.v.s → Då ett medlemskap upphör skall föreningen radera personuppgifterna på begäran
- Om någon vill utöva denna rättighet i en förening innebär det i praktiken att man skriver ut sig ur föreningen. MEN föreningen är självklart inte skyldig att radera uppgifterna om medlemmen vill kvarstå i föreningen. Föreningen kan dessutom ha ett berättigat intresse att spara vissa uppgifter om medlemskapet – måste definieras.

GDPR – den registrerades rättigheter

Artikel 18

Rätt till begränsning av behandling

1. Den registrerade ska ha rätt att av den personuppgiftsansvarige kräva att behandlingen begränsas om något av följande alternativ är tillämpligt:

a) **Den registrerade bestrider personuppgifternas korrekthet**, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta.

b) Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.

c) Den personuppgiftsansvarige behöver inte längre personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

d) Den registrerade har invänt mot behandling i enlighet med artikel 21.1 i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

2. Om behandlingen har begränsats i enlighet med punkt 1 får sådana personuppgifter, med undantag för lagring, endast behandlas med den registrerades samtycke eller för att fastställa, göra gällande eller försvara rättsliga anspråk eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller för skäl som rör ett viktigt allmänintresse för unionen eller för en medlemsstat.

3. En registrerad som har fått behandling begränsad i enlighet med punkt 1 ska underrättas av den personuppgiftsansvarige innan begränsningen av behandlingen upphör.

GDPR – den registrerades rättigheter

Artikel 19

Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett i enlighet med artiklarna 16, 17.1 och 18, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

GDPR – den registrerades rättigheter

Artikel 20

Rätt till dataportabilitet

1. Den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta, om

a) behandlingen grundar sig på samtycke enligt **artikel 6.1 a eller artikel 9.2 a** eller på ett avtal enligt artikel 6.1 b, och

b) behandlingen sker automatiserat.

2 Vid utövandet av sin rätt till dataportabilitet i enlighet med punkt 1 ska den registrerade ha rätt till överföring av personuppgifterna direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt.

3. Utövandet av den rätt som avses i punkt 1 i den här artikeln ska inte påverka tillämpningen av artikel 17. Den rätten ska inte gälla i fråga om en behandling som är nödvändig för att utföra en uppgift av allmänt intresse eller som är ett led i myndighetsutövning som utförs av den personuppgiftsansvarige.

4. Den rätt som avses i punkt 1 får inte påverka andras rättigheter och friheter på ett ogynnsamt sätt

GDPR – den registrerades rättigheter

Artikel 21

Rätt att göra invändningar

1. Den registrerade ska, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på **artikel 6.1 e eller f**, inbegripet profilering som grundar sig på dessa bestämmelser. Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk.

2. Om personuppgifterna behandlas för direkt marknadsföring ska den registrerade ha rätt att när som helst invända mot behandling av personuppgifter som avser honom eller henne för sådan marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring.

3. Om den registrerade invänder mot behandling för direkt marknadsföring ska personuppgifterna inte längre behandlas för sådana ändamål.

GDPR – den registrerades rättigheter

- 4. Senast vid den första kommunikationen med den registrerade ska den rätt som avses i punkterna 1 och 2 uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från eventuell annan information.
- 5. När det gäller användningen av informationssamhällets tjänster, och trots vad som sägs i direktiv 2002/58/EG, får den registrerade utöva sin rätt att göra invändningar på automatiserat sätt med användning av tekniska specifikationer.
- 6. Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, ha rätt att göra invändningar mot behandling av personuppgifter avseende honom eller henne om inte behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

GDPR – den registrerades rättigheter

Artikel 22

Automatiserat individuellt beslutsfattande, inbegripet profilering

1. Den registrerade ska ha rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.

2. Punkt 1 ska inte tillämpas om beslutet

a) är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige,

b) tillåts enligt unionsrätten eller en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av och som fastställer lämpliga åtgärder till skydd för den registrerades rättigheter, friheter och berättigade intressen, eller

c) grundar sig på den registrerades uttryckliga samtycke.

3. I fall som avses i punkt 2 a och c ska den personuppgiftsansvarige genomföra lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen, åtminstone rätten till personlig kontakt med den personuppgiftsansvarige för att kunna utrycka sin åsikt och bestrida beslutet.

4. Beslut enligt punkt 2 får inte grunda sig på de särskilda kategorier av personuppgifter som avses i artikel 9.1, såvida inte artikel 9.2 a eller g gäller och lämpliga åtgärder som ska skydda den registrerades berättigade intressen har vidtagits.

GDPR – ansvar

- Art 24: **Den personuppgiftsansvariges ansvar**
  - 1.Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige **genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning**. Dessa åtgärder ska ses över och uppdateras vid behov.
  - 2.Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.
  - 3.Tillämpningen av godkända uppförandekoder som avses i artikel 40 eller godkända certifieringsmekanismer som avses i artikel 42 får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter.

GDPR – ansvarig & biträde

- Art 25 **Inbyggt dataskydd och dataskydd som standard**
  - 1.Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, **både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder** – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas.
  - 2.Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.
  - 3.En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

GDPR – ansvarig & biträde

- Art 28 **Personuppgiftsbiträden**
  - 1.Om en behandling ska genomföras på en personuppgiftsansvarigs vägnar ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som **ger tillräckliga garantier** om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i denna förordning och säkerställer att den registrerades rättigheter skyddas.
  - 2. Personuppgiftsbiträdet **får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige**. Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgiftsbiträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

GDPR – ansvarig & biträde

- *Art 33* **Anmälan av en personuppgiftsincident till tillsynsmyndigheten**
  - 1.Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, **såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.** Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.
  - 2.Personuppgiftsbiträdet ska underrätta den personuppgiftsansvarige utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident.
  - (info om vad anmälan ska innehålla i Art 33.3)
    - Anmälan får ges i omgångar om inte möjligt att ge den samtidigt

  - *Personuppgiftsincident* = en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats (Art 4.12)

GDPR – ansvarig & biträde

- Art 34 **Information till den registrerade om en personuppgiftsincident**
  - 1.Om personuppgiftsincidenten sannolikt leder till en **hög risk för fysiska personers rättigheter och friheter** ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.
  - 2. Den information till den registrerade som avses i punkt 1 i denna artikel ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och åtminstone de upplysningar och åtgärder som avses i artikel 33.3 b, c och d.
  - 3. Information till den registrerade i enlighet med punkt 1 krävs inte om något av följande villkor är uppfyllt:
  - a) Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.
  - b) Den personuppgiftsansvarige har vidtagit ytterligare åtgärder som säkerställer att den höga risk för registrerades rättigheter och friheter som avses i punkt 1 sannolikt inte längre kommer att uppstå.
  - c) Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

GDPR - Rättsmedel, ansvar och sanktioner

- Art 77 **Rätt att lämna in klagomål till en tillsynsmyndighet**
  - 1. Utan att det påverkar något annat administrativt prövningsförfarande eller rättsmedel, ska varje registrerad som anser att behandlingen av personuppgifter som avser henne eller honom strider mot denna förordning ha rätt att lämna in ett klagomål till en tillsynsmyndighet, särskilt i den medlemsstat där han eller hon har sin hemvist eller sin arbetsplats eller där det påstådda intrånget begicks.

GDPR - Rättsmedel, ansvar och sanktioner

- Art 82: **Ansvar och rätt till ersättning**
  - 1.Varje person som har lidit materiell eller immateriell skada till följd av en överträdelse av denna förordning ska ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan.

GDPR - Rättsmedel, ansvar och sanktioner

- Art 83.5 Vid överträdelser av följande bestämmelser ska det i enlighet med punkt 2 påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:
  - a) De grundläggande principerna för behandling, inklusive villkoren för samtycke, enligt artiklarna 5, 6, 7 och 9.
  - b) Registrerades rättigheter enligt artiklarna 12–22.
  - c) Överföring av personuppgifter till en mottagare i ett tredjeland eller en internationell organisation enligt artiklarna 44–49.
  - d) Alla skyldigheter som följer av medlemsstaternas lagstiftning som antagits på grundval av kapitel IX.
  - e) Underlåtenhet att rätta sig efter ett föreläggande eller en tillfällig eller permanent begränsning av behandling av uppgifter eller ett beslut om att avbryta uppgiftsflödena som meddelats av tillsynsmyndigheten i enlighet med artikel 58.2 eller underlåtelse att ge tillgång till uppgifter i strid med artikel 58.1.
- 6.Vid underlåtenhet att rätta sig efter ett föreläggande från tillsynsmyndigheten i enlighet med artikel 58.2 ska det i enlighet med punkt 2 i den här artikeln påföras administrativa sanktionsavgifter på upp till 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

GDPR - Rättsmedel, ansvar och sanktioner

- Men, obs – lång rad faktorer som kan inverka, ex. överträdelsens karaktär, svårighetsgrad, varaktighet, om det skett med uppsåt eller genom oaktsamhet, hur man samarbetet med myndigheten, om godkända uppförandekoder eller certifieringar har tillämpats etc. etc.
- D.v.s. → ingen automatik

Undantag

- Register över behandlingen (art. 30)
  - Behövs inte ifall:
    - Ett företag eller en organisation sysselsätter färre än 250 personer såvida inte den behandling som utförs sannolikt kommer att medföra risk för registrerades rättigheter och friheter, behandlingen inte är tillfällig eller behandlingen omfattar särskilda kategorier av uppgifter

Undantag

- Utnämning av dataskyddsombud (avs. 4, art. 37-39)
  - Dataskyddsombud skall utses ifall
    - b) den personuppgiftsansvariges eller personuppgiftsbiträdets **kärnverksamhet** består av behandling som, på grund av sin karaktär, sin omfattning och/eller sina ändamål, kräver **regelbunden och systematisk övervakning av de registrerade i stor omfattning**, eller
    - c) den personuppgiftsansvariges eller personuppgiftsbiträdets **kärnverksamhet** består av **behandling i stor omfattning av särskilda kategorier av uppgifter** i enlighet med artikel 9 och personuppgifter som rör fällande domar i brottmål och överträdelser, som avses i artikel 10 (art. 37.1.b-c)
  - Det är klart att merparten av föreningar inte uppfyller dessa kriterier och således inte är skyldiga att utse ett dataskyddsombud.

Dataskyddslagen

Dataskyddslagen

- I Finland har en lag stiftats för att komplettera GDPR; Dataskyddslagen
- Lagen upphäver (bl.a.) personuppgiftslagen
- Lagen trädde i kraft 1.1.2019

Dataskyddslagen

- Laglig behandling (bl.a. arkivering)
- Åldersgräns för barn
- Behandling av personbeteckning
- Tystnadsplikt
- Strafflagen: dataskyddsbrott
- Mest; om övervakningsmyndighetens verksamhet

Dataskyddslagen

- 4§: Personuppgifter får behandlas i enlighet med artikel 6.1 e i dataskyddsförordningen, om
  - 1) det är fråga om uppgifter som beskriver en persons ställning samt uppdrag och skötseln av detta inom ett offentligt samfund, näringslivet, organisationsverksamhet eller någon annan motsvarande verksamhet, i den mån som **syftet med behandlingen är förenligt med allmänt intresse och behandlingen står i proportion till det legitima mål som eftersträvas**,
  - 2) behandlingen behövs och är proportionell i en myndighets verksamhet för utförande av en uppgift av allmänt intresse,
  - 3) behandlingen behövs för vetenskaplig eller historisk forskning eller för statistikföring och den står i proportion till det mål av allmänt intresse som eftersträvas, eller
  - 4) behandling av forskningsmaterial och kulturarvsmaterial som innehåller personuppgifter samt av personuppgifter som hänför sig till innehålls- och referensinformation som gäller sådant material behövs för arkivändamål och behandlingen står i proportion till det mål av allmänt intresse som eftersträvas och den registrerades rättigheter.
- (Art 6.1.e: Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.)
  - Dataskyddslagen 4§ anger alltså när art 6.1.e kan åberopas.

Dataskyddslagen – barn

- När personuppgifter behandlas med samtycke enligt artikel 6.1 a i dataskyddsförordningen och det är fråga om informationssamhällets tjänster enligt artikel 4.25 i dataskyddsförordningen som erbjuds direkt till ett barn, är behandlingen av barnets personuppgifter lagenlig, om barnet är minst 13 år.

Personbeteckning

- 29§: En personbeteckning får behandlas med den registrerades samtycke eller när behandlingen regleras i lag. Dessutom får en personbeteckning behandlas, om det är viktigt att entydigt särskilja den registrerade och den registrerades personuppgifter från andra registrerade och deras personuppgifter (*specificering*)
- 1) för att utföra en i lag angiven uppgift,
- 2) för att tillgodose den registrerades eller den personuppgiftsansvariges rättigheter och uppfylla den registrerades eller den personuppgiftsansvariges skyldigheter, eller
- 3) för historisk eller vetenskaplig forskning eller för statistikföring.
- En personbeteckning får behandlas för entydig specificering av den registrerade vid kreditgivning och indrivning av fordringar, i försäkrings-, kreditinstituts-, betaltjänst-, uthyrnings- och utlåningsverksamhet, i kreditupplysningsverksamhet, inom hälso- och sjukvården, inom socialvården och inom annan verksamhet för att tillförsäkra social trygghet samt i ärenden som gäller tjänste- och arbetsavtalsförhållanden och andra anställningsförhållanden och förmåner som har samband med dessa.
- Utöver vad som i 1 och 2 mom. föreskrivs om behandling av personbeteckningar får en personbeteckning lämnas ut för sådan databehandling som sker i syfte att uppdatera adressuppgifter eller undvika mångfaldig postning, om mottagaren redan har tillgång till personbeteckningen.
- En personbeteckning får inte onödigtvis antecknas i handlingar som skrivs ut eller upprättas på basis av ett register.
- Enbart personbeteckningen eller en kombination av personbeteckningen och den registrerades namn får inte användas för utredning av den registrerades identitet med hjälp av uppgifter som den registrerade har uppgett eller lämnat eller med hjälp av handlingar som den registrerade har visat upp (*identifiering*).

Anställda

- 30§: Bestämmelser om behandling av anställdas personuppgifter, test och kontroller som anställda ska genomgå och de krav som ställs på dessa, teknisk övervakning på arbetsplatsen samt hämtning och öppnande av anställdas e-postmeddelanden finns i lagen om integritetsskydd i arbetslivet (759/2004).

Tystnadsplikt

- 35§: Den som vid utförandet av åtgärder som har samband med behandlingen av personuppgifter har fått kännedom om något som gäller en annan persons egenskaper, personliga förhållanden, ekonomiska ställning eller någon annans företagshemligheter får inte obehörigen för utomstående röja de uppgifter som han eller hon erhållit på detta sätt eller använda uppgifterna för sin egen eller någon annans vinning eller för att skada någon annan.

Guide: Behandling av personuppgifter i föreningsverksamhet

- Dataombudsmannen har publicerat en guide som gäller föreningar och GDPR.
- Positivt att en guide har skrivits
  - Tolkningarna är tämligen maximalistiska och tar inte ställning till uttryckliga bestämmelser i GDPR, ex. 9.2.d eller bestämmelsen om överföring inom en koncern.
  - Guiden antyder att ”ett register över behandlingen” behövs – vilket inte är fallet i majoriteten av föreningar.
- Men, guiden är nyttig och kan gärna studeras – trots att som alltid då det gäller GDPR är svaret oftast, det beror på…
- Antyder hur DO kan tänkas ställa sig i situationer där en förening är part hos myndigheten.

Guide: Behandling av personuppgifter i föreningsverksamhet

- Vilka personuppgifter om medlemmar får en förening behandla?
- Får föreningar använda personbeteckning i medlemsuppgifterna?
- Får en förening behandla frågor om medlemmarnas religiösa övertygelse, hälsa eller politiska åsikter?
- Får en förening behandla andra än medlemmars personuppgifter (t.ex. kunders)?
- Får en föreningsmedlems uppgifter utlämnas till andra medlemmar?
- Får en idrottsförening publicera tävlingsresultat?
- Får en idrottsförening ge frivilliga funktionärer uppgifter om barn (t.ex. namn,födelseår, hemort), som coachas av funktionären?
- Kan en centralorganisation behandla lokala medlemsföreningars personuppgifter?
- Kan en förening outsourca behandlingen av personuppgifter?
- Kan en förenings kommunikation delvis betraktas som direktmarknadsföring?
- Hur länge ska en förenings medlemsuppgifter förvaras?

Vad ska vi göra?

To Do-lista

- Analys av personuppgifter, processer, risker och säkerhet – **dokumentera skriftligen förberedelsearbetet, t.ex. genom att protokollföra (vad, vem, när, hur etc).** Gå igenom alla sammanhang som föreningen behandlar personuppgifter i (t.ex. medlemsregistret, kontaktregister, anmälningar etc.) och känsliga/förbjudna uppgifter.
- Fastställ rättslig grund för alla kontexter ni behandlar personuppgifter. För varje kontext måste man kolla att det finns en laglig grund (i praktiken "rättsliga förpliktelser", "berättigat intresse" eller "samtycke", från artikel 6)
  - Bestäm hur ni hanterar eventuella moment där **samtycke** krävs → Dokumentera
- Beakta principerna för behandling. Säkerställ att föreningen för varje kontext uppfyller principerna för behandling (från artikel 5)
  - Vad innebär principerna i praktiken? Hur konkretiseras de? → Dokumentera
- Garantera den registrerades rättigheter
  - Skapa dokument på basis av **Artikel 13** och bestäm hur den informationen ges till den registrerade
  - Kolla också att ni kan garantera rätten till tillgång enligt artikel 15 (delvis samma info som i artikel 13)
- Beakta regleringen då registertjänster köps in
- Anteckna de åtgärder som föreningen behöver vidta och följ sedan under kommande styrelsemöten upp att sakerna blir åtgärdade
- Gå t.ex. en gång per år med styrelsen igenom föreningens GDPR-arbete; är alla dokument uppdaterade? Är processerna i skick?
- Dokumentera, skriv ned, protokollför och följ upp – räcker inte att skriva, konkreta dokumenterade åtgärder är nyckeln

Artikel 13: modell

- En normal förening med sedvanlig verksamhet kan alltså ha ett dokument i stil med följande:
  - OBS! Information enligt artikel 13 bör finnas tillhanda för alla sammanhang där en förening hanterar personuppgifter. Denna modell är uppgjord enbart med tanke på medlemsregistret. Men det går också att skriva ett dokument som gäller all hantering av personuppgifter. Å andra sidan hanteras personuppgifter i många sammanhang som det inte är relevant att nämna i en allmän offentlig beskrivning, tex. anställda. Eftersom ”registerbeskrivning” är ett vedertaget begrepp kan det användas, men obs att det är föråldrat. ”Dataskydd” används ofta som allmän beteckning.
  - Notera också att den här informationen skall tillställas den vars uppgifter samlas in i samband med att de samlas in (art. 13.1: ”när uppgifterna erhålls”).

- Ex: www.sls.fi/sv/dataskydd/

Artikel 13: modell

- (Röd text är avsedd att anpassas)

- **<u>Registerbeskrivning / Dataskydd / Information enligt artikel 13 i GDPR</u>**

- **Föreningens namn och kontaktuppgifter**
  - Förening X rf, webbadress, e-postadress, telefonnummer

Artikel 13: modell

- **Medlemsregistrets ändamål och den rättsliga grunden**
  - Medlemsregistrets ändamål är att möjliggöra och dokumentera föreningens verksamhet och organisation samt att förverkliga föreningens stadgeenliga syfte och skydda föreningens och medlemmarnas rättigheter och skyldigheter. Komplettera vid behov.
  - Den rättsliga grunden för medlemsregistret är GDPR artikel 6.1.c (rättsliga förpliktelser) och 6.1.f (berättigat intresse). Beträffande nationell lagstiftning finns stadganden i föreningslagen och bokföringslagen. Komplettera vid behov med andra lagar.
- Berättigat intresse
  - Föreningens berättigade intresse består av nödvändigheten att behandla vissa grundläggande uppgifter med beaktande av GDPR artikel 5 som hänför sig till medlemskapet, att förverkliga föreningens stadgeenliga syfte, att förverkliga och skydda föreningens och medlemmens rättigheter och skyldigheter samt att kunna hålla kontakt med medlemmen och att kunna dokumentera föreningens verksamhet. Komplettera utgående från eget fall.

Artikel 13: modell

- **Mottagare av personuppgifterna**
  - Personuppgifterna hanteras av föreningens styrelse, medlemssekreterare, kassör och bokförare. Uppgifterna är även tillgängliga för anställda vid Förbund Y rf. Uppgifterna i medlemsregistret överlämnas inte utöver till förbundet utanför organisationen.

- **Lagringsperioden**
  - Uppgifterna lagras så länge som medlemskapet fortgår och raderas därefter.

Artikel 13: modell

- **Rättigheter**
  - Personer som finns upptagna i medlemsregistret har rätt att begära tillgång till och rättelse av sina uppgifter. Så länge medlemskapet fortgår är det inte möjligt att begära radering av sina uppgifter eller att begränsa eller invända mot behandlingen. Rätten till dataportabilitet är med stöd av artikel 20.1.a och 20.1.b inte möjlig att utöva.

Artikel 13: modell

- **Klagomål**
  - Personer som finns upptagna i medlemsregistret har rätt att inge klagomål till Dataombudsmannens byrå.

- **Skyldighet att tillhandahålla uppgifter**
  - Föreningslagen förutsätter att föreningen upprätthåller en förteckning över samtliga medlemmar. Ifall uppgifterna inte lämnas är det inte möjligt att vara medlem i föreningen.

Frågor?

- Länkar:
  - https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng GDPR
  - https://tietosuoja.fi/sv/vanliga-fragor-foreningsverksamhet DO:s guide
  - https://www.finlex.fi/sv/lagstiftning/1989/503 Föreningslagen
  - https://www.finlex.fi/sv/lagstiftning/2018/1050 Dataskyddslagen

  - För att verkligen förstå är det bäst att läsa hela GDPR.

  - **Fritt fram att ta kontakt med frågor: sebastian@fsu.fi**