Riktlinjer för behandling av personuppgifter

Remeo

Innehållsförteckning

Syfte ... 3
Tillämpningsområde ... 4
Definitioner ... 4
Befogenheter och ansvarsområden ... 5
Beskrivning ... 5
- När får vi behandla personuppgifter enligt GDPR? ... 5
- Vad är en nödvändig behandling? ... 5
  - Hantering av samtycke och återkallelse ... 7
  - Avtal ... 7
  - Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse ... 7
- Behandlingen är nödvändig för att skydda intressen ... 8
  - Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse. ... 8
- Laglig grund känsliga personuppgifter ... 8
  - Checklista ... 8
- Chefer och HR ... 10
  - Rekryteringsprocessen ... 10
  - Personuppgifter till fackliga organisationer och skyddsombud ... 10
  - Behandling av personnummer/samordningsnummer ... 10
- Hur ska personuppgifter hanteras? ... 11
  - Lagligt, skäligt och öppet. ... 12
  - Ändamålet sätter gränser ... 12
  - Så få personuppgifter som möjligt ... 13
  - Personuppgifterna ska vara korrekta ... 13
  - Personuppgifterna ska inte sparas längre än nödvändigt ... 13
  - Personuppgifterna ska skyddas mot obehöriga ... 13
- Organisationen ska kunna visa att man följer GDPR ... 13
- Behövs konsekvensbedömning? ... 14
- Information om verksamhetens hantering av personuppgifter ... 14

Allmänt om information till den registrerade 14
Information när pu samlas in från den enskilde (artikel 13) 14
Information när personuppgifter samlas in från annan än den registrerade 16
Undantag från informationsskyldigheten: 16
Begäran om utdrag över personuppgifter 16
Samling, registrering, inhämtande, organisering, bearbetning, användning, ändring, lagring 16
Inbyggt skydd och säkerhet för personuppgifter 16
Skydd för personuppgifterna är utgångspunkten. 17
Lagringsytor 19
Personuppgifter på G: 19
Personuppgifter på U: 19
Personuppgifter på C: 19
Behandling av personuppgifter i Outlook, Skype och mobilen 19
Hantering av foton 20
Behandling på webben och internet 20
Molntjänster och överföring av personuppgifter till tredje land 21
Arkivering 21
Artikel 30 22
Rättelse, radering, begränsning och invändning mot behandling av personuppgifter 22
Begäran om rättelse av personuppgift 22
Rättelse sker inte om 22
Skyldighet att anmäla rättelse 22
Om verksamheten får en begäran om radering av personuppgifter 23
Kontrollera att uppgifterna kan raderas 23
Skyldighet att anmäla radering och underrättelse om radering 24
Organisationen får en begäran om begränsning av behandling 24
En enskild har i vissa fall rätt att invända mot behandling av dennes personuppgifter. 24
Gör en prövning och behandlingen upphör eller fortsätter 24
Motsättning mot automatiserade beslut 25
Undantag från reglerna i GDPR 25
Utanför tillämpningsområdet 25
Brottsdatalag 26
Patientdatalagen 26
Intergritetslagarna 27
Versionshistorik 27

Syfte

Denna rutin vänder sig till alla medarbetare inom organisationen i frågor som rör verksamhetens behandling av personuppgifter. Rutinen förklarar regelverket i dataskyddsförordningen (EU) 2016/679, (GDPR), och ger praktiska råd och instruktioner i fråga om behandlingen av personuppgifter. Rutinen ska vara en hjälp i det vardagliga arbetet för alla medarbetare när man hanterar personuppgifter.

Rutinen är också ett sätt att visa att verksamheten följer GDPR. I anslutning till denna rutin finns också rutiner för

- vägledning sociala medier
- hantering av registerutdrag

Tillämpningsområde

Tillämpbar inom organisationen för behandling av personuppgifter utanför journalsystem.

Definitioner

Personuppgifter: varje upplysning som självständigt eller med hjälp av andra uppgifter, hos någon annan, kan härledas till en identifierad, levande fysisk person. Namn och personnummer är direkta personuppgifter.

Indirekta personuppgifter kan vara en lokaliseringsuppgift eller en IP-adress. Fastighetsbeteckning, medlemsnummer eller anställningsnummer är (indirekta) person-uppgifter. Likaså foto och ljudupptagning, om man kan identifiera personerna i fråga.

Känsliga personuppgifter: personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Integritetskänsliga personuppgifter: personuppgifter som är integritetskänsliga även om de inte faller inom kategorin känsliga personuppgifter. Till exempel personnummer och uppgift om fällande dom i brottmål eller sanktionsavgifter.

Behandling: all hantering av personuppgifter 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.

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.

Personuppgiftsbiträde: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Samtycke av den registrerade: en frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, godtar behandling av personuppgifter som rör honom eller henne.

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.

Artikel 29-gruppen: Arbetsgrupp som består av en företrädare för varje nationell tillsynsmyndighet i EU-medlemsstaterna, en företrädare för EU- kommissionen samt den europeiske datatillsynsmannen. Gruppen är rådgivande och ska bl.a. se till att EU:s regelverk om dataskydd tillämpas enhetligt i medlemsstaterna. Gruppen kommer genom GDPR att ersättas av europeiska dataskyddsstyrelsen.

Dataskyddsombud: Ombudets roll regleras uttryckligen i GDPR. Dataskyddsombudet ska objektivt kontrollera att dataskyddsförordningen följs inom den aktuella organisationen, samt ge råd, utbilda och informera.

Befogenheter och ansvarsområden

Alla som behandlar personuppgifter inom organisationen.

Beskrivning

När får vi behandla personuppgifter enligt GDPR?

Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. De specifika ändamål som personuppgifterna behandlas för bör vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Det innebär att organisationen måste ha ändamålen klara för sig redan innan insamlingen av personuppgifter börjar. Om det inte är organisationen som samlar in personuppgifterna utan dessa kommer in, t ex via e-post från allmänheten, krävs på samma sätt att organisationen vet för vilket ändamål som den fortsatta behandlingen av personuppgifterna sker.

Ändamålet ska vara berättigat i förhållande till grundlag, annan lag och även omständigheterna i det aktuella fallet.

Personuppgifterna får inte behandlas på ett sätt som är oförenligt med det eller de angivna ursprungliga ändamålen. De på förhand fastställda ändamålen sätter ramarna för behandlingen.

Ändamålen ska dokumenteras skriftligt och den registrerade ska få information om ändamålen både när uppgifterna samlas in och annars när denne begär det. Om de insamlade personuppgifterna senare ska behandlas för andra ändamål som är förenliga med de ursprungliga ändamålen, måste de registrerade också informeras om detta.

De insamlade personuppgifterna får behandlas för arkivändamål av allmänt intresse eller statistiska ändamål utan att det anses oförenligt med de ursprungliga ändamålen. Enligt dataskyddslagen finns dock begränsningar för hur personuppgifter som behandlas för dessa ändamål får användas gentemot den registrerade, se 4 kap. dataskyddslagen.

För att behandla personuppgifter lagligt krävs att som personuppgiftsansvarig har en rättslig grund för sin behandling enligt artikel 6.

Behandling av personuppgifter är endast laglig om och i den mån som åtminstone ett av villkoren i artikel 6.1.a-f är uppfyllt. För behandling av särskilda kategorier av personuppgifter (”känsliga personuppgifter”), måste även villkoren i artikel 9 iakttas, se Laglig grund, känsliga

personuppgifter. Förutom rättslig grund krävs dessutom alltid att behandlingen sker i överensstämmelse med hanteringsprinciperna i artikel 5.

Vad är en nödvändig behandling?

Förutom när det gäller grunden samtycke, krävs det för övriga rättsliga grunder att behandlingen av personuppgifter ska vara nödvändig för att uppfylla respektive rättslig grund i artikel 6.

Behandlingen ska vara nödvändig för att fullgöra, skydda eller utföra den rättsliga grunden i fråga.

Att en behandling är nödvändig kan innebära att den rättsliga skyldigheten överhuvudtaget inte kan fullgöras, skyddas eller utföras utan att behandlingen sker. Men begreppet ”nödvändig” i GDPR täcker även in de fall där en uppgift inte är absolut nödvändig.

Frågan om en behandling är nödvändig kan utfalla olika beroende på syftet och på vilken form av behandling det gäller, dvs insamling, registrering, utlämnande, samkörning osv. Det måste bedömas om varje behandlingssteg för sig är nödvändigt.

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

Samtycke kan inte betraktas som frivilligt om den registrerade inte har någon verklig valmöjlighet eller inte utan problem kan vägra eller ta tillbaka sitt samtycke.

Samtycke anses därför inte utgöra giltig rättslig grund för behandling av personuppgifter i fall där det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige, särskilt om den personuppgiftsansvarige är en offentlig myndighet.

När organisationen agerar som arbetsgivare är frågan om samtycke också problematisk på grund av det ojämlika förhållandet mellan anställd och arbetsgivare. Som huvudregel kan en arbetsgivare inte använda sig av samtycke som rättslig grund för behandling av personuppgifter, eftersom samtycket inte kan anses lämnat frivilligt. Detta innebär dock inte att det är uteslutet för en arbetsgivare att grunda behandling av personuppgifter på ett samtycke från en anställd. För att det ska vara möjligt måste samtycket dock verkligen vara frivilligt, vilket innebär att den anställde ska ha en reell valmöjlighet och det ska inte finnas någon risk för att den anställde upplever tvång (t ex genom att ett nekande medför extra arbete eller kostnader för arbetsgivaren).

Samtycke ska finnas innan personuppgifterna börjas behandlas. Samtycke ska lämnas genom en entydig bekräftande handling som innebär ett frivilligt, specifikt, informerat och otvetydigt medgivande från den registrerades sida om att denne godkänner behandlingen av personuppgifter rörande honom eller henne. Detta kan ske både genom en skriftlig och en muntlig förklaring. Samtycke bör som huvudregel hanteras i skriftlig form.

Samtycke kan inbegripa att en ruta kryssas i vid besök på en internetsida, genom val av inställningsalternativ för e-tjänster eller något annat beteende som i sammanhanget tydligt visar att den registrerade godtar den avsedda behandlingen av sina personuppgifter. Samtycket ska kunna särskiljas från eventuellt andra frågor.

För giltigt samtycke krävs en entydig bekräftande handling. I vissa fall kan därför samtycke ges genom en aktiv handling i sig, dvs ett agerande som konstituerar ett samtycke. Ett exempel är att den som skickar ett mail med vissa personuppgifter därmed också samtycker till att organisationen får behandla uppgifterna genom att ta emot mailet. Men där slutar också samtycket. GDPR kräver i detta avseende dessutom att personuppgiftsansvarig lämnar tillräcklig information om på vilket sätt och för vilka syften som personuppgifter i e-post behandlas.

Information som ges till den enskilde i samband med inhämtande av samtycke ska vara i en begriplig och lätt tillgänglig form, med klart och tydligt språk. Se mer under Information till den registrerade.

Tystnad, på förhand ikryssade rutor eller inaktivitet utgör inte samtycke. Samtycket bör gälla all behandling som utförs för samma ändamål. Om behandlingen tjänar flera olika syften, behöver samtycke ges för samtliga olika syften.

Den registrerade ska när som helst återkalla sitt samtycke, och fortsatt behandling av personuppgifterna på den grunden blir då olaglig.

Det finns två utarbetade mall-texter för samtycke, som sedan får anpassas till varje enskilt fall.

Hantering av samtycke och återkallelse

Eftersom organisationen ska kunna visa att giltigt samtycke lämnats, bör samtycke som huvudregel hanteras i skriftlig form. Lämnade samtycken ska hållas ordnade. Samtycken som lämnas via webbformulär ska kopplas till mailkorgen för den medarbetare som är ansvarig för samtyckena. Denne ska spara samtyckena i en för ändamålet skapad mapp på enhetens G:. Mappen bör endast vara tillgänglig för de som jobbar med samtyckena i fråga.

Ett samtycke kan återkallas även muntligt. Efter en återkallelse får några ytterligare uppgifter om den registrerade inte samlas in eller annars behandlas, inom ramen för den behandling som omfattas av samtycket.

Organisationen kan trots ett återkallat samtycke genomföra sådan behandling som är nödvändig för att förhindra att ytterligare personuppgifter om den registrerade behandlas. Det kan t.ex. gälla registrering av en uppgift om att den registrerade återkallat sitt samtycke och att ytterligare personuppgifter därför inte får behandlas.

Avtal

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.

Som exempel på behandling som kan vara nödvändig för att fullgöra ett avtal kan nämnas fakturering, kundregister och förandet av kundkonton.

Sådana bestämmelser i kollektivavtal mellan arbetsgivare eller organisation av arbetsgivare och fackförening som anses flyta in i det enskilda anställningsavtalet mellan arbetsgivare och arbetstagare får anses ingå i det avtalet, medan andra bestämmelser i kollektivavtalet inte i sig kan grunda någon rätt för kollektivavtalsparterna att behandla personuppgifter.

Personuppgifter får behandlas om det är nödvändigt för att anställningsavtalet eller något annat avtal mellan arbetsgivaren och arbetstagaren ska kunna uppfyllas. Av anställningsavtalet följer att organisationen får behandla en rad personuppgifter om den anställde, så som namn, personuppgifter, etc. För att uppfylla anställningsavtalet behövs även behandla personuppgifter om den anställde på sätt som krävs för att t ex kunna betala ut lön, för att den anställde ska kunna komma in på arbetsplatsen (in- och utpasseringssystem) etc.

Åtgärder som vidtas innan ett avtal träffas på begäran av den registrerade kan vara kontroller av olika slag. Om en arbetssökande lämnar uppgifter om referenspersoner, får det t ex anses vara en sådan begäran som berättigar den tilltänkte arbetsgivaren att hämta in personuppgifter om den som söker tjänsten från referenspersonerna.

Det är inte sannolikt att ett avtal med en registrerad skulle kunna berättiga en personuppgifts-ansvarig att behandla uppgifter om andra än just avtalsparten.

Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse

Det framgår av GDPR att även syftet med behandlingen måste vara fastställt i den rättsliga grunden. Detta innebär att den författning eller det beslut som reglerar en rättslig skyldighet inte kan vara alltför vag i fråga om den behandling av personuppgifter som är nödvändig för att fullgöra den rättsliga skyldigheten. Som exempel kan nämnas att ett företags skyldighet att lämna uppgift om företagets lönekostnader inte innehåller något angivet syfte för behandling av personuppgifter i form av utlämnande. Om skyldigheten däremot innebär att företaget behöver lämna uppgifter om löneutbetalning till vissa arbetstagare, så finns ett syfte, eftersom denna förpliktelse i praktiken inte kan uppfyllas utan att personuppgifter rörande arbetstagarna behandlas.

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

Av GDPR framgår att behandling av personuppgifter bör anses laglig när den är nödvändig för att skydda ett intresse som är av avgörande betydelse för den registrerades eller en annan fysisk persons liv. Vidare anges att behandling av personuppgifter på grundval av en annan fysisk persons grundläggande intressen i princip endast bör äga rum om behandlingen inte uppenbart kan ha en annan rättslig grund. Detta innebär alltså att behandling enligt denna grund endast i undantagsfall kan ske av personuppgifter som tillhör någon annan än den vars vitala intressen ska skyddas. Även om den registrerade uttryckligen motsätter sig personuppgiftsbehandlingen, får den utföras för att kunna skydda vitala intressen för den registrerade. Detta kan bli aktuellt vid tvångsvård. Det kan också vara så att den enskilde inte kan lämna samtycke p g a sitt hälsotillstånd och behöver vård akut, vilket i sin tur kräver att dennes personuppgifter behandlas.

Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

Behandlingen är nödvändig för ändamål som rör verksamheten 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.

Det kan vara tillåtet att behandla personuppgifter efter en intresseavvägning. Det krävs då att behandlingen är nödvändig för berättigade intressen och att den registrerades intresse av skydd för sina personuppgifter inte väger tyngre. Intressen som har att göra med säkerhetsskäl har ansetts i allmänhet väga tyngre än intressen som rör företagsekonomiska effektivitetsskäl. Uppgifternas karaktär har en avgörande betydelse vid intresseavvägningen.

Denna grund kan användas när organisationen agerar som arbetsgivare, eftersom detta faller utanför fullgörande av sina uppgifter. I dessa fall måste dock särskilt beaktas att arbetsgivare och arbetstagare inte har ett jämbördigt förhållande.

Laglig grund känsliga personuppgifter

Känsliga personuppgifter enligt artikel 9 är uppgifter om

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening

- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter och
- biometriska uppgifter som entydigt identifierar en person

Det är förbjudet att behandla känsliga personuppgifter utom i uttryckligt reglerade fall, bland annat

- om behandlingen av personuppgifterna är nödvändig för att organisationen eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina rättigheter på arbetsrättens område

- Hantering av personuppgifter inom hälsa och sjukvård under sekretess
- Förutom rättslig grund enligt Dataskyddsförordningens artikel 9 måste rättslig grund enligt artikel 6 alltid finnas.
- Hanteringsprinciperna ska alltid följas.
- Känsliga personuppgifter som behandlas med stöd av arbetsrätten får lämnas ut till tredje man endast om det enligt arbetsrätten finns en skyldighet att göra det.
- Undantag finns i fråga om behandling för arkivändamål av allmänt intresse och statistiska ändamål.
- Personuppgifter som rör fällande domar i brottmål har ett extra skydd i GDPR, även om de inte kategoriseras som känsliga och skall skötas av myndigheter.

Utgångspunkten är att det är förbjudet att behandla känsliga personuppgifter. Det finns dock en rad undantag som möjliggör behandling av känsliga personuppgifter i vissa fall. Den registrerade kan i de flesta fall samtycka till att sådan behandling sker. Samtycket ska då vara uttryckligt.

Ett av undantagen är att känsliga personuppgifter får behandlas om behandlingen är nödvändig för att organisationen eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och inom områdena social trygghet och socialt skydd. I begreppet arbetsrätt inryms också kollektivavtal.

Personuppgifter som behandlas med stöd av denna rättsliga grund får enligt dataskyddslagen lämnas ut till tredje part endast om det inom arbetsrätten finns en skyldighet att göra det, eller om den registrerade uttryckligen har samtyckt till utlämnandet.

I stort sett alla skyldigheter och rättigheter för en arbetsgivare beträffande de anställda bör kunna omfattas av regleringen att organisationen eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten. Ett exempel är den behandling som sker i samband med sjuklön och rehabilitering av arbetstagare. Även skyldigheter och rättigheter för fackliga organisationer och skyddsombud i förhållande till arbetsgivare innefattas. Se mer under Chefer & HR.

Uppgifter om fällande dom i brottmål skyddas genom att det i regel endast är myndigheter som får behandla sådana uppgifter.

Chefer och HR

Anställdas personuppgifter behandlas av organisationen för en rad olika ändamål. Av anställningsavtalet framgår vad dessa ändamål är, den lagliga grunden för behandlingen samt övrig information enligt artikel 13 i GDPR. I vissa undantagsfall kan organisationen behandla anställdas personuppgifter även med stöd av samtycke.

Sjukintyg. Både chefer och HR hanterar känsliga personuppgifter om hälsa. Hanteringen av sådana personuppgifter ställer särskilt höga krav på att tillgången till personuppgifterna begränsas och att uppgifterna hålls säkra.

Läkarintyg ska enligt interna arbetssätt lämnas till chefen, som omgående ska lämna intyget vidare till utsedd medarbetare på lönefunktionen på personalenheten. Chefen behöver tänka på att uppgifterna är känsliga och rekommenderas att alltid lämna över sjukintyget i ett kuvert. När den anställde lämnar sjukintyg till sin chef ska detta inte ske via e-post, utan sjukintyget ska överlämnas till chefen i pappersform eller skickas per post.

Observera att det i tillägg till de lagliga grunderna i artikel 6 krävs särskilda grunder enligt artikel 9 för att få behandla känsliga personuppgifter.

Varken chef eller HR får spara sjukintyg längre tid än vad som krävs utifrån ändamålen med behandlingen. Om personuppgifter i ett sjukintyg behandlas utifrån grunden att det krävs för att fullgöra en arbetsrättslig skyldighet, ska sjukintyget slängas när den arbetsrättsliga skyldigheten uppfyllts. Att spara ett sjukintyg för att det kan komma att behövas i ett eventuellt framtida rehabiliteringsärende är inte förenligt med GDPR. Om ett rehabiliteringsärende uppstår, får sjukintyg i så fall ges in på nytt i den mån det krävs.

Rekryteringsprocessen

Tänk på att reglerna om ändamålsbegränsning, laglig grund och hanteringsprinciperna i övrigt också gäller för de personuppgifter som hanteras inom ramen för rekryteringsprocessen. I samband med att kandidater skickar in sin ansökan får de information om att de genom sin ansökan samtycker till att organisationen behandlar deras personuppgifter i syfte att ta ställning till deras ansökan om anställning. Behandlingen av de sökandes personuppgifter kan därför endast ske för detta syfte. Det är chefens ansvar att inte sprida CV och ansökan till andra än de som anses nödvändiga för processen. Chefen måste tänka på om det är nödvändigt att medarbetare tar del av CV/ansökan, exempelvis om de är behjälpliga vid urval eller inför möte med slutkandidater. CV/ansökan ska inte sparas på andra ställen än i mapp eller rekryteringsprogram. I den mån CV/ansökan skickas med e-post ska e-posten raderas.

Personuppgifter till fackliga organisationer och skyddsombud

Organisationen är enligt arbetsrätten, dvs kollektivavtal, samverkansavtal eller lagstiftning skyldig att lämna vissa uppgifter till företrädare för de fackliga organisationerna och skyddsombuden. När uppgifterna lämnats övergår ansvaret för behandlingen av personuppgifterna till de fackliga organisationerna. Därför är det viktigt att fackliga företrädare och skyddsombud har tillräcklig kunskap om GDPR och följer de riktlinjer som lämnas centralt av deras respektive organisationer.

Behandling av personnummer/samordningsnummer

Personnummer och samordningsnummer får behandlas utan samtycke bara om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Behandlingen av personnummer och samordningsnummer ska alltså vara restriktiv och ska föregås av en intresseavvägning mellan behovet av behandlingen och de integritetsrisker som den innebär. Regleringen innefattar givetvis även att en uppgift om personnummer får behandlas t.ex. genom att fästas på en utskrift eller visas upp på en datorskärm bara när den behandlingen är klart motiverad med hänsyn till något beaktansvärt skäl.

Detta innebär att man även i ärendehantering inte alltid behöver ha personnummer, om det inte är nödvändigt för en säker identifiering.

Personnummer ska som utgångspunkt inte användas som användaridentitet vid inloggning.

Som arbetsgivare kan t ex registrera personnummer för att administrera sina anställda eller för att kunna lämna uppgifter till olika myndigheter, till exempel Skatteverket. Däremot finns det sällan anledning att använda personnummer när man skriver ut tjänstgöringslistor etc.

Hur ska personuppgifter hanteras?

- **Laglighet, skälighet och öppenhet**

  Behandlingen ska ha en laglig grund, vara skälig i förhållande till den registrerade och information om behandlingen ska ges den enskilde.

- **Ändamålsbegränsning**

  Innan behandlingen av personuppgifter påbörjas ska det finnas ett tydlig angivet syfte med behandlingen. Syftet ska framgå i register över personuppgiftsbehandlingar.

  Personuppgifterna får inte behandlas för något annat ändamål än det ursprungliga ändamålet, om det är oförenligt med det ursprungliga ändamålet.

- **Uppgiftsminimering**

  Personuppgifter ska endast behandlas i den mån som de är relevanta i förhållande till syftet med behandlingen. Om uppgifterna inte behövs utifrån ändamålet ska de raderas eller avidentifieras.

- **Korrekthet**

  Personuppgifterna ska vara korrekta och uppdaterade. Personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas ska rättas utan dröjsmål.

- **Lagringsminimering**

  Personuppgifter ska raderas eller avidentifieras när de inte längre behövs i förhållande till det ändamål för vilket de behandlas.

  Undantag gäller för t ex arkivändamål av allmänt intresse. Uppgifter ska inte behandlas på fler ställen än nödvändigt utifrån ändamålet.

- **Integritet och konfidentialitet**

  Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, så som skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Lämpliga tekniska eller organisatoriska åtgärder ska vidtas.

- **Ansvarsskyldighet**

  Organisationen ska som personuppgiftsansvarig kunna visa att hanteringsprinciperna och andra centrala delar av GDPR efterlevs.

Lagligt, skäligt och öppet.

Att behandlingen ska vara laglig innebär att det måste finnas en laglig grund för behandlingen, men att också eventuella andra krav på legalitet är uppfyllda. Om vi saknar ett legitimt ändamål för behandlingen utifrån sitt uppdrag kan behandlingen av personuppgifter inte vara laglig.

Behandlingen ska vara rättvis och skälig gentemot den enskilde – även om det finns en laglig grund enligt artikel 6 ska en behandling inte vidtas om den uppfattas som oskälig i förhållande till den enskilde.

Att personuppgifter ska behandlas på ett öppet sätt i förhållande till den registrerade innebär bland annat att det ska vara klart och tydligt för denne hur hans eller hennes personuppgifter samlas in och i övrigt behandlas. De registrerade måste därför få information om behandlingen som är både lättillgänglig och formuleras med ett klart och tydligt språk. Se Information till den registrerade.

Ändamålet sätter gränser

Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. När det ska behandla personuppgifter måste verksamheten alltså ha ändamålen klara för sig redan innan insamlingen eller behandlingen i övrigt av personuppgifter börjar. Det är inte tillåtet att samla in personuppgifter för obestämda framtida behov.

Personuppgifter får inte behandlas på ett sätt som är oförenligt med de ursprungliga ändamålen (finalitetsprincipen). De på förhand fastställda ändamålen är med andra ord det som sätter ramarna för behandlingen. Ändamålen ska dokumenteras skriftligt och den registrerade ska få information om ändamålen både när uppgifterna samlas in och annars när denne begär det. Se Information till den registrerade.

För att bedöma om en behandling är förenlig med det ursprungliga ändamålet ska man beakta bland annat:

- kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen,
- det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan den registrerade och organisationen,
- personuppgifternas art, särskilt om känsliga personuppgifter enligt artikel 9 behandlas eller om annars integritetskänsliga personuppgifter behandlas,
- eventuella konsekvenser för den registrerade av den planerade fortsatta behandlingen,
- vilka skyddsåtgärder som kan vidtas, vilket kan inbegripa kryptering eller pseudonymisering.

De insamlade personuppgifterna får behandlas för arkivändamål av allmänt intresse och statistiska ändamål utan att det anses oförenligt med de ursprungliga ändamålen.

Så få personuppgifter som möjligt

Endast de uppgifter som är adekvata och relevanta för ändamålet får samlas in eller på annat sätt behandlas. Personuppgifterna får alltså inte vara för omfattande i förhållande till ändamålet med behandlingen.

Personuppgifterna ska vara korrekta

Personuppgifterna ska vara korrekta och uppdaterade. Organisationen måste vidta alla rimliga åtgärder för att säkerställa att felaktiga personuppgifter raderas eller rättas utan dröjsmål.

Personuppgifterna ska inte sparas längre än nödvändigt

Insamlade personuppgifter får förvaras i en form som möjliggör identifiering av den registrerade bara så länge som det är nödvändigt i förhållande till ändamålen för behandlingen.

När personuppgifterna inte längre är nödvändiga utifrån ändamålen ska de raderas eller avidentifieras. För att säkerställa att personuppgifter inte sparas längre än nödvändigt är det viktigt att tidsfrister och rutiner finns för radering eller avidentifiering av personuppgifter. Tidsfrister för radering av uppgifter finns i dokumenthanteringsplanen Dessa tidsfrister gäller också för uppgifter i de olika systemen.

De insamlade personuppgifterna får lagras under längre tid än vad som krävs utifrån det ursprungliga ändamålet, om detta sker för arkivändamål av allmänt intresse eller för statistiska ändamål.

Uppgifter ska inte heller behandlas på fler ställen än nödvändigt utifrån ändamålet. Detta innebär att personuppgifter som behandlas för samma ändamål inte ska behandlas på både G:, U:, Outlook etc, utan på så få ställen som möjligt.

Personuppgifterna ska skyddas mot obehöriga

Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna. Personuppgifterna ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Vad som är en lämplig säkerhetsnivå för personuppgifterna beror på bland annat riskerna med behandlingen, vilken typ av uppgifter som behandlas och på de tekniska möjligheter som finns samt på kostnaderna. Tekniska och organisatoriska åtgärder för att uppnå säkerhet ska utformas bland annat utifrån den informationsklassning som gjorts för informationsmängden i fråga.

Skydd mot obehörig eller otillåten behandling inom myndigheten ska säkerställas genom åtkomstbegränsning. Endast medarbetare som behöver personuppgifterna i sitt arbete ska ha åtkomst till dessa personuppgifter.

Detta innefattar även läsbehörighet. Se mer under Insamling, registrering, inhämtande, organisering, bearbetning, användning, ändring, lagring

Organisationen ska kunna visa att man följer GDPR

Organisationens ansvarar i egenskap av personuppgiftsansvarig för att principerna om personuppgiftsbehandling följs och måste kunna visa på vilket sätt som de följs.

Det finns flera sätt att visa detta. Till exempel genom tydlig information till de registrerade, genom att dokumentera de behandlingar som pågår och de överväganden man gör samt att ha tydliga

interna regler om dataskydd och se till att reglerna följs. Principen om ansvarsskyldighet genomsyrar dataskyddsförordningen och återfinns på flera ställen. Bland annat anges i artikel 24.1 att den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med GDPR.

Behövs konsekvensbedömning?

Som personuppgiftsansvarig är man skyldig att fortlöpande bedöma den risk som uppkommer vid behandlingen av personuppgifter.

En konsekvensbedömning krävs enligt artikel 35.1 i GDPR om behandlingen ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”.

En konsekvensbedömning kan avse en enda behandling av uppgifter, men kan också användas för att bedöma flera behandlingar som liknar varandra vad gäller art, omfattning, innehåll, ändamål och risker. Syftet med konsekvensbedömningarna är att systematiskt studera behandlingar som utförs i ett särskilt sammanhang och av en särskild anledning, som kan medföra hög risk för fysiska personers rättigheter och friheter.

Om det är osäkert om en konsekvensbedömning är nödvändig bör en konsekvensbedömning ändå utförs, eftersom det är ett användbart verktyg för att hjälpa att iaktta dataskyddslagstiftningen.

Se mer om konsekvensbedömning i Rutin för konsekvensbedömning vid behandling av personuppgifter.

Information om verksamhetens hantering av personuppgifter

Allmänt om information till den registrerade

All kommunikation med den registrerade ska vara tydlig och lättbegriplig. Viss allmän information kan finnas på hemsidan men ofta krävs att information ska lämnas på t ex en blankett eller i ett webbformulär, dvs att informationen lämnas i samband med att personuppgifter samlas in.

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 dock 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 i dessa fall att visa att begäran är uppenbart ogrundad eller orimlig.

Information när pu samlas in från den enskilde (artikel 13)

Den övervägande delen av personuppgifter som behandlas och samlas in eller erhålls från de registrerade själva. Med detta menas

- att den enskilde medvetet lämnar personuppgifter, eller
- att samlar in personuppgifter genom att följa/observera den enskilde, t ex genom att spåra var någons dator eller telefon befinner sig,

Nedan följer vissa kommentarer till kraven på information enligt artikel 13.

Mottagare: Begreppet mottagare inkluderar även de som behandlar personuppgifterna inom organisationen. Artikel 29 gruppen anger i sin vägledning att den personuppgiftsansvarige kan välja att istället för namn ange kategorier av mottagare, dvs vilka enheter som tar emot uppgifterna. I slutändan krävs dock alltid att man vet vilka medarbetare som har behörighet till uppgifterna och behöver dem för sina arbetsuppgifter.

Period som uppgifterna kommer att lagas: Det räcker inte att ange att personuppgifterna kommer att lagras under den tid som är nödvändig utifrån syftet med behandlingen. Organisationen behöver således utifrån varje behandling ta ställning till hur länge uppgifterna ska lagras och sedan arkiveras/när de ska tas bort.

Information om rätten att begära rättelse, tillgång till uppgifterna, radering, begränsning av behandling samt invända mot behandlingen: Informationen ska innehålla en sammanfattning av vad rättigheterna innebär samt på vilket sätt den registrerade kan tillvarata dessa rättigheter.

Om tillhandahållandet är ett lagstadgat eller avtalsenligt krav: I vissa fall behöver verksamheten behandla personuppgifter för att antingen kunna ingå ett avtal eller annars utföra en viss uppgift. Till exempel behövs vissa personuppgifter för att kunna ingå ett anställningsavtal. Informationen ska i dessa fall tydligt ange vilka personuppgifter som är ”obligatoriska” och vad som blir följden av att de inte lämnas. Likaså måste anges i vilka fall som den enskilde är skyldig enligt lag eller avtal att tillhandahålla uppgiften.

Exempel på några situationer som kräver information enligt artikel 13:

Anställningsavtal: Information om de behandlingar som är generella för alla medarbetare ska finnas i avtalet.

Information till konsulter: Eftersom organisationen inte ingår avtal med enskilda konsulter som privatpersoner, krävs att konsulter ges information i samband med att uppdraget påbörjas.

Anmälningar till konferenser, föreläsningar och liknande: Information enligt artikel 12 ska finnas i webbformuläret eller på pappersblanketten, om sådan används.

Ansökningar eller anmälningar som görs till genom webbformulär eller blankett: Information enligt artikel 12 ska finnas i webbformuläret eller på pappersblanketten, om sådan används.

E-post: Informationstext ska finnas på hemsidan samt en kort text i själva e-postmeddelandet med länk till hemsidan, se ovan.

Webbtjänster, så som Mina sidor, etc: Information ska finnas på hemsidan samt i samband med inloggning till tjänsten.

Information när personuppgifter samlas in från annan än den registrerade

Informationen ska lämnas inom rimlig tid efter det att personuppgifterna erhållits och senast inom en månad. Om personuppgifterna ska användas för kommunikation med den registrerade, ska information lämnas senast vid tidpunkten för den första kommunikationen eller om utlämnande sker till annan mottagare, senast när personuppgifterna lämnas ut för första gången.

Enligt Artikel 29-gruppen ska strävan dock vara att så snart som möjligt och redan innan påbörjad behandling lämna informationen.

Förutom informationen enligt artikel 13 ska även information lämnas om vilka kategorier av personuppgifter som behandlas, dvs vilka kontaktuppgifter, foton, inkomstuppgifter, CV, etc.

Den specifika källan till uppgifterna ska anges såvida det inte saknas möjlighet. Organisationen bör ha en överblick över varifrån personuppgifterna som de behandlar erhålls.

Undantag från informationsskyldigheten:

I de fall som listas nedan behöver information inte ges. Undantagen är följande och bör tolkas restriktivt.

- Den registrerade redan förfogar över informationen.
- Om tillhandahållandet av information till den registrerade visar sig vara omöjligt eller medföra en oproportionell ansträngning, exempelvis i samband med arkivering.
- Om erhållandet/utlämnandet föreskrivs i nationell/EU rätt (exempelvis myndighetsutövning, offentlighetsprincipen). I sådana fall ska det dock finnas information om att organisationen erhåller och lämnar ut personuppgifter i enlighet med lagstiftningen i fråga.
- Det föreligger sekretesshinder för att ovanstående information ska kunna ges till den registrerade. En bedömning måste i så fall göras av om sekretessen hindrar all information enligt artikel 14 eller endast i vissa delar.

Begäran om utdrag över personuppgifter

Den registrerade ska ha rätt att på begäran få information om personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna och viss information.

Se Rutin för registerutdrag över personuppgifter.

Samling, registrering, inhämtande, organisering, bearbetning, användning, ändring, lagring

Reglerna om rättslig grund i artiklarna 6 och 9 samt hanteringsprinciperna i artikel 5 gäller oavsett om personuppgifterna behandlas i en egenutvecklad databas, i Outlook eller på G:. Av principen om integritet och konfidentialitet följer att vidta de åtgärder som behövs för att skydda personuppgifterna.

Inbyggt skydd och säkerhet för personuppgifter

Inbyggt dataskydd innebär att man tar hänsyn till integritetsskyddsreglerna redan när man utformar IT-system och rutiner. Det är ett sätt att se till att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas. Vid egenutvecklade system ska organisationen beakta denna princip och redan vid utvecklingen anpassa behörighetsstruktur, möjlighet till loggning osv till den nivå som krävs utifrån arten av personuppgifter som behandlas.

Fritextfält i system bör undvikas eftersom vilka personuppgifter som helst kan skrivas in, oavsett om de är relevanta eller inte. Om fritextfältet behövs, bör det finnas en text i anslutning till fältet som informerar om att endast de personuppgifter som behövs i sammanhanget ska skrivas in.

Verksamheten ska ha en lämplig säkerhetsnivå för personuppgifterna som behandlas, både tekniskt och organisatoriskt. Vad som är en lämplig säkerhetsnivå beror på bland annat riskerna

med behandlingen, vilken typ av uppgifter som behandlas, på de tekniska möjligheter som finns och på kostnaderna.

Vid riskbedömningen ska särskild hänsyn tas till de risker som behandlingen medför, i synnerhet risken för 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.

Pseudonymisering och kryptering av personuppgifter är exempel på åtgärder som minskar risken med behandlingen. Pseudonymiserade personuppgifter kan inte kopplas till en specifik individ utan att man använder kompletterande information. Den kompletterande informationen måste förvaras tekniskt och organisatoriskt avskild så att personuppgifterna inte kan hänföras till en person.

Skydd för personuppgifterna är utgångspunkten.

Dataskydd som standard innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Detta innebär till exempel att personuppgifter i system och lagringsytor som utgångspunkt ska vara stängda, och sedan göras tillgängliga för enbart de som behöver uppgifterna i sitt arbete.

Nedan listas några särskilt viktiga hållpunkter i fråga om dataskydd som standard.

Skyddade personuppgifter ska sekretessmarkeras. För att obehöriga inte ska komma åt skyddade personuppgifter ska det finnas sekretessmarkeringar som syns tydligt vid sökningar i register/system. De medarbetare som kan komma att hantera skyddade personuppgifter ska ges utbildning om skyddade personuppgifter och sekretessfrågor. Kretsen av personer som har tillgång till skyddade personuppgifter ska begränsas så mycket som möjligt.

En differentierad behörighet till personuppgifter är grundläggande för att skydda personuppgifterna mot t ex obehörig åtkomst. Behörighetsstruktur ska finnas oavsett var personuppgifterna lagras.

Det är ansvarig informationsägare för varje system som beslutar om behörighet för en anställd ska beviljas och på vilken nivå. Avgörande är om medarbetaren behöver tillgång till personuppgifterna i fråga för att kunna utföra sitt arbete. Skäl som att det kan vara bra att ha åtkomst, eller att det är mindre jobbigt än att i ett enskilt fall begära tillgång till uppgifterna, är inte tillräckliga skäl.

Även om man som medarbetare tekniskt har behörighet till vissa uppgifter, innebär detta inte att man enligt GDPR får behandla dem. Varje behandling av personuppgifter måste göras för ett berättigat ändamål som har sin grund i verksamheten. Det innebär bland annat att man inte får söka efter personuppgifter av privata skäl eller annars, om detta inte är nödvändigt för arbetsuppgifterna.

Inaktivering av externa behörigheter. Rensning ska ske av användardatabas varje månad och då inaktivera alla konton som inte har används på ett år. Detta gäller alla konton. Det är IT-avdelningen som ansvarar för inaktiveringen av konton.

Inaktivering av interna behörigheter. När medarbetare slutar sin anställning ska medarbetarens användarkonton och behörigheter tas bort. Det är medarbetarens chef som utan dröjsmål ska anmäla till IT- avdelningen att medarbetaren slutat.

Apple ID: Anställda måste använda ett Apple ID för att kunna använda sin arbetstelefon. När ett sådant konto upprättas, behöver den enskilde lämna en e-postadress, vilket är en personuppgift. För att privata personuppgifter inte ska skickas till Apple, ska medarbetare som får en telefon uppge sin företagsadress.

Testdata/utvecklingsdata. Verkliga personuppgifter får användas i test- och utvecklingsmiljöer endast om det finns en laglig grund för en sådan användning och hanteringsreglerna ska då följas.

För just test- och utvecklingsdata behöver man särskilt se till att personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in och att inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen.

I denna bedömning får man utgå från hur en registrerad typiskt sett skulle se på saken. Om den aktuella behandlingen rimligen kunde förväntas av den registrerade är det nya ändamålet inte att anse som oförenligt med det ursprungliga.

Behandling i test- eller utvecklingsmiljö som görs för att säkerställa att de uppgifter som finns i produktion behandlas på ett korrekt sätt och för att upptäcka och korrigera felaktiga personuppgifter har ett naturligt samband med det ursprungliga syftet med behandlingen, dvs att tillhandahålla den ifrågavarande tjänsten. En sådan behandling i testmiljö bör därför i allmänhet inte anses oförenligt med den ursprungliga behandlingen.

Systemtester bör så långt det är möjligt utföras på ett sätt som inte innebär att personuppgifter behandlas. I de fall verkliga personuppgifter används är det viktigt att inte fler personuppgifter behandlas än de som är nödvändiga för att utföra det aktuella testet. Personuppgifter får inte heller bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Personuppgifter som används för teständamål bör därför gallras en relativt kort tid efter behandlingen slutförts.

När personuppgifter behandlas i testmiljön gäller samma regler för behandling som när det är fråga om behandling som sker i produktionsmiljön. Detta innebär att rutiner i fråga om behörigheter, loggar, loggkontroller och IT-säkerhet ska gälla även för personuppgifter som behandlas i testmiljön.

Testmiljö och produktionsmiljö ska vara tydligt åtskilda och vidta nödvändiga åtgärder för att förhindra att testhandläggare av misstag utför åtgärder i produktionsmiljön avseende en verklig person. En sådan åtgärd är att det finns tydlig varningstext när man länkar testmiljö till produktionsmiljön.

Mer om detta finns i rutin för databasstandard på enheten för systemutveckling på IT-avdelningen.

Loggning i systemen. För att skydda personuppgifterna och för att undvika att oskyldiga misstänks om några oegentligheter skulle inträffa, behöver det finnas loggning av aktiviteter i system. Detta gäller såväl egenutvecklade som inköpta system. I egenutvecklade verksamhetssystem ska alla aktiviteter som behandlar personuppgifter loggas.

Vid behov kan IT avdelningen genom loggningen säkerställa att tilldelade behörigheter är korrekta och används korrekt och kan utreda eventuella personuppgiftsincidenter.

Loggar över aktiviteter ska sparas i 90 dagar.

Lagringsytor

Personuppgifter på G:

Det får inte finnas mappar på G: utan någon ansvarig medarbetare. Denna medarbetare ansvarar för innehållet och kontroll av innehål . Eftersom hanteringsprinciperna gäller även för personuppgifter på G: ska man ha ett berättigat ändamål med behandlingen av personuppgifter på G:, så som en tydlig koppling till arbetet. Man ska minimera antalet personuppgifter och

undvika dubbletter. På G: krävs en tydlig mappstruktur och behörighetsstyrning, detta regleras genom FORM-xxxx behörighetsmatris och ansvar…

Personuppgifter på U:

U: (hemkatalogen) ska användas för att spara varje medarbetares eget arbetsmaterial. Var och en bygger upp U: utifrån den struktur som önskas. Varje medarbetare ansvarar för att skapa en sådan struktur som tillåter att personuppgifter kan tas bort när de inte längre behövs etc. Eftersom hanteringsprinciperna gäller även för personuppgifter på U: ska man ha ett berättigat ändamål med behandlingen av personuppgifter på U:, så som en tydlig koppling till arbetet. Man ska minimera antalet personuppgifter och undvika dubbletter.

Personuppgifter på C:

C: är en lokal hårddisk som inte säkerhetskopieras. Dokument får inte sparas på C: eftersom någon back-up inte sker av C:.

Behandling av personuppgifter i Outlook, Skype och mobilen

- Tänk på för vilka ändamål du behandlar personuppgifter i e-posten. Ändamålen styr vilken laglig grund som kan finnas. Oftast är det frågan om att det är nödvändigt att skicka e-post för att arbetet ska kunna fortgå.
- Mängden personuppgifter ska alltid minimeras till det som är nödvändigt utifrån syftet med behandlingen.
- För att minimera personuppgifter i mailen eller i kalendern – skicka en länk istället för att bifoga dokument.
- Skriv inte personuppgifter i ämnesraden för e-posten eller bokningen.
- Skriv aldrig in känsliga eller på annat sätt integritetskänsliga personuppgifter i ämnesraden eller bokningen.
- Personuppgifter som är känsliga ska inte skickas externt med okrypterad e-post.
- För personliga förhållanden, ska krypteras när de överförs i öppna nätverk som exempelvis internet.
- Skicka e-post bara till de som behöver ta del av personuppgifterna utifrån sina arbetsuppgifter.
- För över e-post till de lagringsytor där e-posten hör hemma.
- Rensa regelbundet e-post som inte längre behövs för dina arbetsuppgifter.
- Det sker en automatisk tömning av mappen borttaget i Outlook en gång i veckan.
- Samma regler gäller även för behandling av personuppgifter som sker i Skype och i tjänstemobilen.
- Skype-historik raderas automatiskt 1 gång i veckan.

Begränsa användningen av personuppgifter i e-post till vad som är nödvändigt för att uppfylla ändamålen med behandlingen av personuppgifter i e-posten. Detta följer av principen om uppgiftsminimering och innebär att man aktivt ska tänka på och bli mer restriktiva när det gäller användning av personuppgifter i e-post. Skriv inte personuppgifter i ämnesraden om det inte är nödvändigt för syftet, och skriv aldrig in känsliga eller integritetskänsliga personuppgifter där.

Tänk på vilka som behöver ta del av e-post som innehåller personuppgifter. Som huvudregel ska bara sådana personer som har behov av tillgång till personuppgifter för att kunna utföra sitt arbete också ha tillgång till dem.

Som ett led i uppgifts- och lagringsminimeringen har organisationen rutiner för återkommande radering av e-post. Det sker en automatisk tömning av mappen borttaget i Outlook en gång i veckan, dvs när e-posten är 7 dagar gammal.

Arbetet med informationssäkerhet omfattar även e-postsystemet. Av rutinen för informationsskydd framgår att integritetskänsliga personuppgifter inte får skickas som okrypterad e-post över öppna nät som internet. Behöver sådana uppgifter skickas med e-post ska de skyddas på ett sådant sätt att obehöriga inte kan ta del av uppgifterna. Även till myndigheter och externa parter som t.ex. banker gäller att e-post innehållande integritetskänsliga personuppgifter ska skickas via en överenskommen lösning för säker e-post. Detta innefattar åtgärder som till exempel att se till att skydda e-posten från obehörig åtkomst från utomstående, att införa tydliga krav på användarnamn och lösenord och så vidare.

Skype-konversation ska ses som ett samtal. Skype-historik raderas automatiskt 1 gång i veckan, dvs när Skype konversation blir 7 dagar gammal raderas det i borttaget.

Samma regler gäller även för behandling av personuppgifter i mobiltelefonen. För över personuppgifter där de gör hemma. Om ett foto tagits i tjänsten, ska det föras över till H:, G:, eller det ärende det tillhör. Samma gäller sms som erhålls i tjänsten. Radera sms och eventuella foton när dessa förts över till andra lagringsytor samt när personuppgifterna inte längre behövs utifrån ändamålet. Behandla inte känsliga personuppgifter i sms.

Hantering av foton

Behandling på webben och internet

Verksamheten måste följa integritetsskyddsreglerna i GDPR vid publicering av personuppgifter på internet. Det innebär bland annat att det måste finnas en laglig grund och ett berättigat ändamål med publiceringen.

Personuppgifter får publiceras när de har samband med personens tjänsteutövning eller uppdrag. Sådana personuppgifter kan till exempel vara uppgift om ansvarig chef, kontaktperson för information eller liknande.

Organisationen ska inte publicera följande på webben:

- Känsliga personuppgifter och uppgifter som omfattas av sekretessbestämmelser till skydd för enskilds personliga förhållanden
- Integritetskänsliga uppgifter så som uppgifter om enskilds personliga förhållanden eller sådant som har en nära koppling till den enskildes privata sfär
- Personnummer eller samordningsnummer

- Uppgift om lagöverträdelse

Se mer i Rutin för hantering av personuppgifter på internet.

Molntjänster och överföring av personuppgifter till tredje land

En molntjänst är en form av outsourcing som innebär att en tjänst tillhandahålls över internet. Exempel på molntjänster är Dropbox, Evernote , Microsoft Office 365.

Riskerna med en molntjänst är att organisationen kan förlora kontrollen över de uppgifter som överförs via internet, eftersom molntjänstleverantören ofta använder sig av underleverantörer. Detta innebär i sin tur en risk för att uppgifter exponeras för andra länders rättsordningar och i övrigt inte åtnjuter tillräckligt skydd, om de förs över till tredje land. Även molntjänstleverantören kan komma att använda sig av servrar utanför EU.

Innan en molntjänst kan användas behöver en laglighetsprövning ske utifrån sekretess och GDPR. Organisationen bör också allmänt pröva om det är lämpligt att en outsourcing sker.

Lämplighetsprövningen sker dels utifrån uppgifterna i sig, även om dessa inte omfattas av sekretess eller utgör känsliga personuppgifter, och dels utifrån vad det är som uppdragstagaren ska göra.

Molntjänster kräver personuppgiftsbiträdesavtal.

Se Rutin för informationsskydd för mer information om molntjänster och vad som gäller om man vill använda en sådan tjänst.

Arkivering

Behandling av personuppgifter som utförs för att uppfylla krav på bevarande för andra syften än att vårda en del av det svenska kulturarvet, såsom exempelvis kravet på arkivering av räkenskapsinformation enligt bokföringslagen (1999:1078), utgör inte behandling för arkivändamål av allmänt intresse. Däremot kan det finnas skäl att bevara även sådan information för arkivändamål av allmänt intresse, t.ex. för att arkivlagen kräver det.

Enligt 6 § dataskyddslagen får känsliga personuppgifter behandlas för arkivändamål av allmänt intresse, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv. Med föreskrifter om arkiv avses föreskrifter som säkerställer att sådana arkiv som utgör en del av det svenska kulturarvet bevaras, hålls ordnade och vårdas. Sådana föreskrifter finns i arkivlagen och arkivförordningen samt i Riksarkivets och andra arkivmyndigheters föreskrifter. Regelverket i GDPR hindrar alltså inte att tex myndigheter bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet.

Artikel 30

Enligt artikel 30 i GDPR ska verksamheten föra ett register över behandlingar som utförts under dess ansvar. Detta register ska innehålla en rad upplysningar om respektive behandling, bland annat ändamålen med behandlingen, kategorierna av registrerade och kategorierna av personuppgifter, de mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter, en allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärder som vidtagits.

Även upplysning om bland annat laglig grund för behandlingen och en beskrivning av i vilka system som behandlingen sker.

Registret är ett av de främsta redskap för att säkerställa att verksamheten följer GDPR och även kan visa att detta sker, i enlighet med principen om ansvarsskyldighet. Det är genom listan som vi vet ändamål, laglig grund, hur länge uppgifterna sparas, vem de skickas till, osv. Till exempel kan listan utgöra underlag till den information som måste ges till de registrerade inför insamling och behandling av personuppgifter. Det är också utifrån listan som man kan bedöma för vilka ändamål som man kan behandla personuppgifterna i fråga, eftersom ändamålen med behandlingen anges i registret.

Listan måste hållas uppdaterad om den ska kunna tjäna sitt syfte. Av arbetsordningen framgår att samtliga enheter ska utse en kontaktperson gentemot dataskyddsombudet i frågor som rör personuppgiftsbehandling inom sina ansvarsområden. Denna kontaktperson ska anmäla nya eller ändrade ändamål och behandlingar till dataskyddsombudet.

Dataskyddsombudet ska också fortlöpande stämma av innehållet i med enhetens representanter.

Rättelse, radering, begränsning och invändning mot behandling av personuppgifter

Begäran om rättelse av personuppgift

Fördjupningstext: Varje person har rätt att vända sig till organisationen och be att få felaktiga uppgifter rättade. Det innebär också att den enskilde har rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen. Detta fråntar givetvis inte organisationen från ansvaret att själv se till att uppgifterna är korrekta och uppdaterade, enligt de grundläggande principerna i dataskyddsförordningen.

Rättelse sker inte om

Om organisationen kommer fram till att rättelse inte ska ske, ska ett skriftligt beslut fattas och skickas till den enskilde. Av beslutet ska framgå att det kan överklagas.

Skyldighet att anmäla rättelse

Om uppgifter rättas på den enskildes begäran måste organisationen också informera dem som verksamheten har lämnat ut uppgifter till om att uppgifter rättats. Det gäller dock inte om det skulle visa sig omöjligt eller innebär en alltför betungande insats. Den enskilde har också rätt att begära och få information om till vem uppgifter har lämnats ut.

Om verksamheten får en begäran om radering av personuppgifter

Rätten att ”bli bortglömd” är central i dataskyddsförordningen. Varje person har rätt att vända sig till verksamheten och be att uppgifterna som avser honom eller henne raderas.

Rätten att bli bortglömd är inte absolut, men personuppgifterna måste raderas i följande fall:

- Om uppgifterna inte längre behövs för de ändamål som de samlades in för
- Om behandlingen grundar sig på den enskildes samtycke och denne återkallar samtycket
- Om den enskilde motsätter sig personuppgiftsbehandling som sker inom ramen för myndighetsutövning eller efter en intresseavvägning och det inte finns berättigade skäl som väger tyngre än den enskildes intresse

- Om personuppgifterna har behandlats olagligt
- Om radering krävs för att uppfylla en rättslig skyldighet

Kontrollera att uppgifterna kan raderas

Det finns undantag från rätten till radering och skyldigheten att informera andra vid offentliggörande, om det är nödvändigt för att tillgodose andra viktiga rättigheter som till exempel rätten till yttrande- och informationsfrihet, för att uppfylla en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

Radering kan ske

Informationsägaren beslutar efter samråd med dataskyddsombudet.

Efter beslut skapas ärende, som tilldelas medarbetare i enlighet med det som gäller för registerutdrag.

Radering får inte ske

Om organisationen kommer fram till att förutsättningar inte finns för att radera uppgifterna, ska ett skriftligt beslut fattas och skickas till den enskilde. Av beslutet ska framgå att det kan överklagas till allmän förvaltningsdomstol.

Skyldighet att anmäla radering och underrättelse om radering

Om uppgifter har raderats på den enskildes begäran måste organisationen informera också eventuella mottagare om raderingen. Det gäller dock inte om det skulle visa sig omöjligt eller innebär en alltför betungande insats. Den enskilde har också rätt att begära att få information om till vem uppgifter har lämnats ut.

Om det har publicerat eller på annat sätt offentliggjort personuppgifterna (i ett socialt nätverk, ett internetforum eller på en webbsida) räcker det inte alltid att de raderas där. För att stärka "rätten att bli bortglömd" i nätmiljön har rätten till radering därför utvidgats. Organisationen har i sådana fall en skyldighet att på den enskildes begäran vidta rimliga åtgärder för att informera andra som behandlar uppgifterna om att den enskilde begärt att även kopior av eller länkar till uppgifterna tas bort.

Organisationen får en begäran om begränsning av behandling

Enskilda har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas. Med begränsning menas att uppgifterna markeras så att dessa i framtiden endast får behandlas för vissa avgränsade syften.

Rätten till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och begärt rättelse. I sådana fall kan den registrerade även begära att behandlingen av uppgifterna begränsas under tiden uppgifternas korrekthet utreds.

Om behandlingen har begränsats 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.

Informationsägaren beslutar efter samråd med dataskyddsombudet.

Efter beslut skapas ärende, som tilldelas medarbetare i enlighet med det som gäller för registerutdrag. Innan begränsningen upphör ska den enskilde informeras om detta.

Om organisationen kommer fram till att förutsättningar inte finns för att begränsa behandlingen ska ett skriftligt beslut fattas och skickas till den enskilde. Av beslutet ska framgå att det kan överklagas till allmän förvaltningsdomstol.

En enskild har i vissa fall rätt att invända mot behandling av dennes personuppgifter.

Rätten att invända gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning.

Om den enskilde invänder mot behandlingen i sådana fall får den personuppgiftsansvarige endast fortsätta att behandla uppgifterna om det går att visa att det finns tvingande berättigade skäl till att uppgifterna måste behandlas som väger tyngre än den enskildes intressen, rättigheter och friheter eller om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

Gör en prövning och behandlingen upphör eller fortsätter

Informationsägaren beslutar efter samråd med dataskyddsombudet. Efter beslut skapas ärende, som tilldelas medarbetare i enlighet med det som gäller för registerutdrag. Behandlingen upphör genom att organisationen raderar personuppgifterna i fråga. Radering ska dock inte ske i arkiverat material.

Om organisationen kommer fram till att formella förutsättningar inte finns för att den enskildes begäran ska beviljas, eller om det finns tvingande skäl för en fortsatt behandlingen, ska ett skriftligt beslut fattas och skickas till den enskilde. Av beslutet ska framgå att det kan överklagas till allmän förvaltningsdomstol.

Motsättning mot automatiserade beslut

Den enskilde har rätt att inte bli föremål för ett beslut som enbart grundas på någon form av automatiserat beslutsfattande, inbegripet profilering, om beslutet kan ha rättsliga följder för den enskilde eller på liknande sätt i betydande grad påverkar honom eller henne.

Automatiserat beslutsfattande kan till exempel vara ett automatiserat avslag på eller beviljande av en ansökan om en förmån, ett tillstånd etc.

Profilering innebär varje form av automatisk behandling av personuppgifter då uppgifterna används för att bedöma vissa personliga egenskaper, i synnerhet för att analysera eller förutsäga personens arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

Automatiserat beslutsfattande kan vara tillåtet om det är nödvändigt för ingående eller fullgörande av ett avtal mellan den registrerade och den personuppgiftsansvarige eller om den enskilde har gett sitt uttryckliga samtycke. Det kan även vara tillåtet enligt särskild lagstiftning.

Den personuppgiftsansvarige måste informera de registrerade om att automatiserat beslutsfattande används enligt den generella informationsskyldigheten i förordningen.

Automatiserade beslut får, utom i vissa fall, inte grunda sig på känsliga personuppgifter.

Undantag från reglerna i GDPR

Undantag görs från flera behandlingsprinciper och även i vissa andra fall i fråga om behandling för arkivändamål av allmänt intresse, statistik och journalistiska ändamål. Relevanta undantag behandlas i respektive avsnitt.

Arkivlagens bestämmelser utgör arkivändamål av allmänt intresse, se under Arkivering.

Med statistiska ändamål avses varje åtgärd som vidtas för den insamling och behandling av personuppgifter som är nödvändig för statistiska undersökningar eller för framställning av statistiska resultat. Ett statistiskt ändamål innebär att resultatet av behandlingen inte består av personuppgifter, utan av aggregerade personuppgifter, och att resultatet eller uppgifterna inte används till stöd för åtgärder eller beslut som avser en särskild privatperson.

Det är vanligt att personuppgifter som ursprungligen har samlats in för andra ändamål vidarebehandlas för statistiska ändamål. Sådan vidarebehandling är särskilt gynnad i dataskyddsförordningen. Uppgifter som ursprungligen har samlats in för något annat ändamål kan användas för statistiska ändamål, utan att denna nya behandling anses vara oförenlig med de ursprungliga ändamålen (artikel 5.1 b i GDPR), under förutsättning att lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda personuppgifterna.

Utanför tillämpningsområdet

Brottsdatalagen ska tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Se mer under Brottsdatalag.

Brottsdatalag

Brottsdatalagen genomför direktiv (EU) 2016/680 av den 27 april 2016, det så kallade dataskyddsdirektivet. Brottsdatalagens tillämpningsområde ligger utanför GDPR:s tillämpning, och gäller alltså parallellt med förordningen.

Brottsdatalagen ska tillämpas på behandling av personuppgifter som utförs i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Det är dock inte tillräckligt att personuppgifterna behandlas i detta syfte. De ska också behandlas av en så kallas behörig myndighet, dvs en myndighet som fullgör arbetsuppgifter inom områdena: förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder.

Patientdatalagen

Reglerna för behandling av personuppgifter inom hälso- och sjukvården finns i patientdatalagen (2008:355), som när den trädde i kraft 2008 ersatte vårdregisterlagen och patientjournallagen. Patientdatalagen ska tillämpas av alla vårdgivare, både i offentlig och privat regi.

Dataskyddsförordningen är direkt tillämplig som svensk lag. Som vårdgivare måste organisationen alltså tillämpa dataskyddsförordningen och kan endast tillämpa den komplett-erande dataskyddslagen och patientdatalagen om de är förenliga med dataskyddsförordningen.

Patientdatalagen reglerar bland annat:

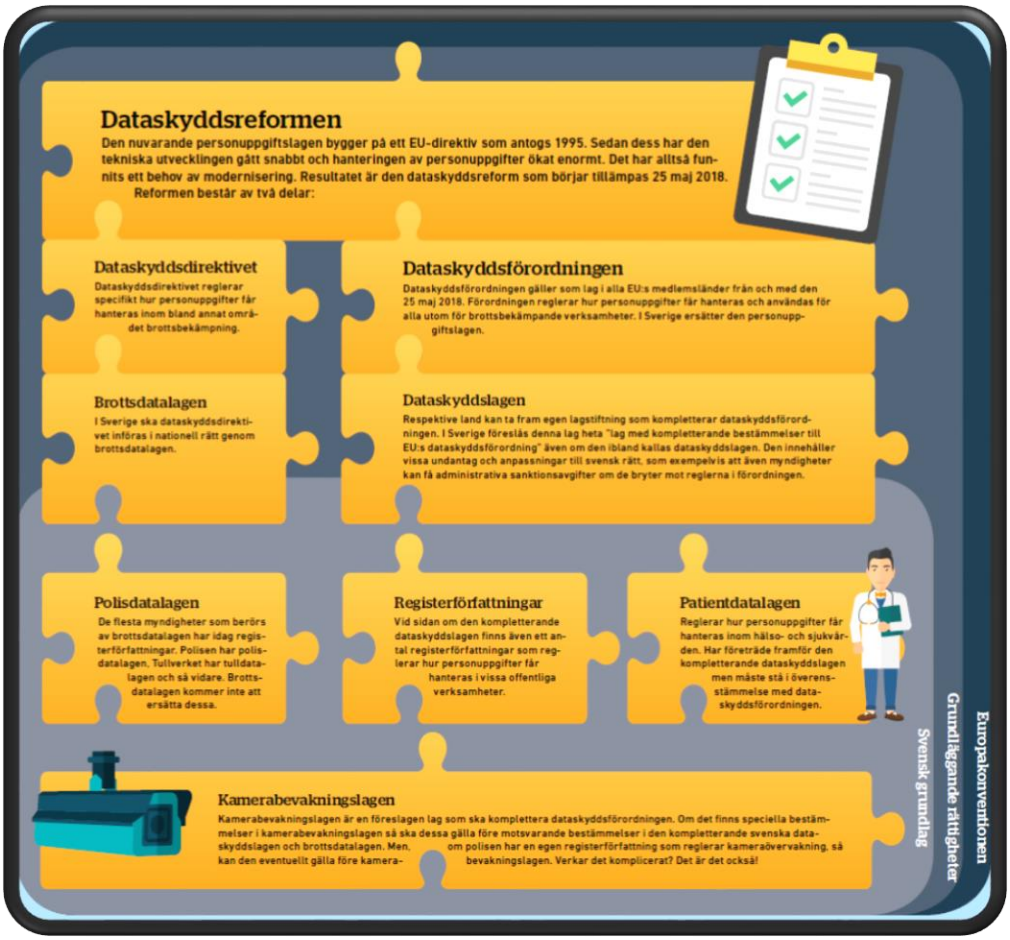
• Vårdgivare har möjlighet att ge patienten direktåtkomst, exempelvis via internet, till patientens vårddokumentation och loggar (det vill säga åtkomsthistoriken för personuppgiftsbehandlingen).

• Sammanhållen journalföring, vilket innebär att flera vårdgivare kan ge och få direktåtkomst till varandras journalhandlingar om de uppfyller patientdatalagens krav.

• Inre sekretess – en reglering som innebär att bara den som behöver uppgifterna i sitt arbete inom hälso- och sjukvården får ta del av patientuppgifter. Detta förtydligas genom att det i lagen ställs krav på behörighetstilldelning och åtkomstkontroll.

• Patienten har rätt att spärra uppgifter både i vårdgivarens journalsystem och för andra vårdgivare vid sammanhållen journalföring.

Intergritetslagarna



Versionshistorik

Datum	Version	Väsentliga ändringar
2018-06-20	1.0	Första publicerade version
2021-06-22		Nytt format