Rädda Barnen

STRATEGI
PROCESS
PLAN
POLICY
▶ RIKTLINJE
RUTIN

RIKTLINJER FÖR PERSONUPPGIFTSBEHANDLING

Fastställda av: Stf generalsekreterare
Datum: 2023-07-11
För revidering ansvarar: Förbundsjurist
Policyn ska uppdateras: 2025-04-30
För uppföljning ansvarar: Generalsekretariatet
Gäller för: Alla anställda samt medlemsrörelsen

Rädda Barnen

RIKTLINJER FÖR PERSONUPPGIFTSBEHANDLING

Rädda Barnen följer GDPR, EU:s dataskyddsförordning, och övrig dataskyddslagstiftning, av vilken framgår hur individers personliga integritet ska skyddas i kontakten med myndigheter, företag och organisationer. Som ett led i detta har Rädda Barnens riksstyrelse antagit en Integritetspolicy som gäller såväl kansli som medlemsrörelse.

Policy

Integritetspolicyn beskriver när och vilka personuppgifter vi samlar in, i vilket syfte de samlas in, på vilket sätt individen kan ha kontroll över dem samt hur hen kan kontakta oss. Policyn gäller i alla sammanhang; när hen besöker vår hemsida, använder sig av någon av våra tjänster där, när hen är med oss på sociala medier eller kommer i kontakt med oss på annat sätt t ex via e-post eller en app som vi står bakom. Policyn gäller även uppgifter vi får in via telefon, post eller om hen lämnar uppgifter till oss på annat sätt.

Integritetspolicy gäller oavsett om en person kommer i kontakt med oss som givare, medlem, frivillig eller bara som intresserad av vår verksamhet. Den gäller också de som kommer i kontakt med oss i sin yrkesroll eller som anställd hos oss.

Det är nödvändigt att känna till dess innehåll då nya sätt att ta in personuppgifter eller nya ändamål med behandlingen kan kräva att policyn ändras och berörda individer informeras.

Policyn är vårt främsta verktyg för att se till att varje berörd individ får den information hen har rätt till och behöver för att kunna ha kontroll över sina personuppgifter.

Syfte

Riktlinjerna för personuppgiftsbehandling ger ett närmare stöd för hur vi agerar och bör göra för att följa och leva upp till vår integritetspolicy och de krav som GDPR och annan lagstiftning ställer.

Rädda Barnens lokalföreningar och distrikt är personuppgiftsansvariga för den behandling som sker i den egna föreningen respektive distriktet. Det innebär att lokalföreningar respektive distrikt ansvarar för att behandling sker enligt gällande lagstiftning.

Rädda Barnen som helhet men även lokalföreningar respektive distrikt har en skyldighet att visa att vi har gjort rätt vilket ställer krav på systematisk dokumentation.

Vid bristande efterlevnad riskerar Rädda Barnen sanktionsavgifter som kan uppgå till mellan 2-4 % av årsomsättningen.

Av integritetspolicyn följer att Riksförbundet förser alla lokalföreningar och distrikt med tekniska och organisatoriska lösningar för t ex e-post- och dokumenthantering. Riksförbundet tillhandahåller också riktlinjer och rutiner rörande den praktiska tillämpningen.

Avgränsningar

Nedanstående riktlinjer är avgränsade till att avse personuppgifter. Riktlinjerna gäller dock såväl

Rädda Barnens kansliorganisation som Rädda Barnens lokalföreningar respektive distrikt.

Riktlinjer

Allmänt

Rädda Barnen har en informationssäkerhetspolicy med tillhörande Riktlinjer för samverkan i IT-förvaltning och rutiner. I den beskrivs hur vi skyddar den information som vi hanterar i vår verksamhet. Perspektivet där är Rädda Barnens. Det sätt som Rädda Barnen tekniskt och organisatoriskt skyddar vår information på är en viktig pusselbit i hur vi kan och ska skydda individers integritet, rent tekniskt och organisatoriskt. Vi fortsätter som tidigare men lägger till ett perspektiv - och tittar utifrån den registrerades (den vars personuppgifter vi behandlar) och ser om den tekniska och organisatoriska säkerheten är tillräcklig.

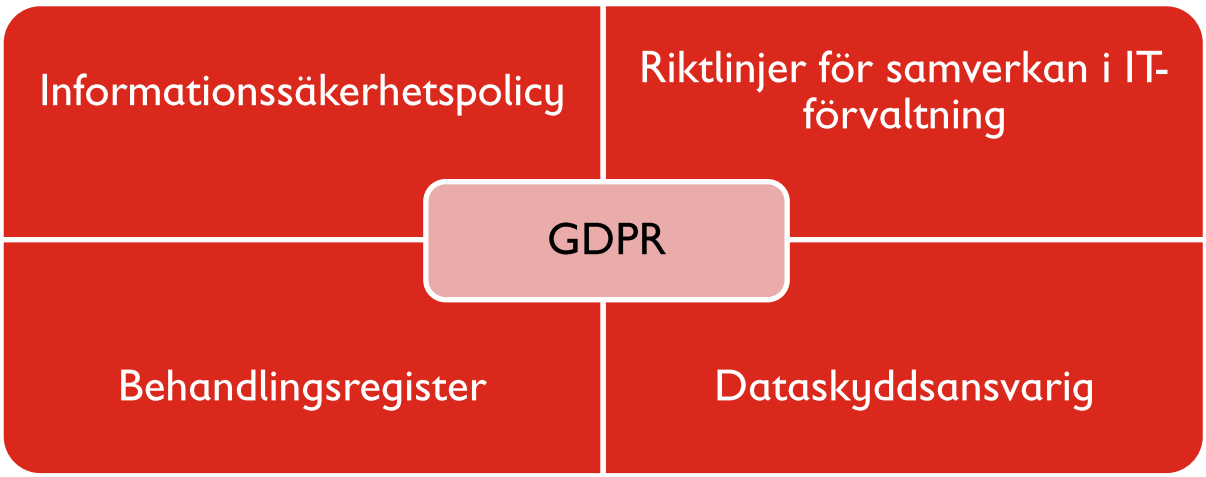
I Riktlinjer för samverkan i IT-förvaltning ges instruktioner till de som är Produktområdesägare, produktägare, processägare samt informationsägare om hur våra Systemstöd, processer och informationsobjekt ska förvaltas. Produktplaner ska tas fram årligen, risk- och konsekvensbedömningar ska göras liksom att information ska klassas. För respektive produktområde ska också nödvändiga rutiner tas fram och hållas uppdaterade. GDPR blir därmed en naturlig del i vårt arbete.

En Informationsägare har det övergripande ansvaret för de informationstillgångar som skapas och används inom en verksamhet. Informationsägaren ska styra produktion, utveckling, underhåll, användning och säkerhet avseende den specifika informationstillgången. I "informationstillgångar" ingår ofta personuppgifter av olika slag. Även här ska nödvändiga rutiner finnas och hållas uppdaterade.

Personuppgifter är en del av all den information vi hanterar och personuppgifter finns nästan över allt och väldigt ofta ensamma (referens i en faktura) eller i kluster (semesterlista/deltagarförteckning) och mer sällan i stora och omfattande system. GDPR träffar *alla* personuppgifter och finns med som en nödvändig del i allas vårt arbete var i organisationen vi än befinner oss.

Det är förklaringen till varför det inte är tillräckligt att få in GDPR i arbetet med processer, information och systemstöd. Det behövs även en överblick och ett ansvarstagande, respektive informationsägare, processägare och produktägare har ansvaret att tillse att GDPR följs. I lokalföreningar respektive distrikt är det styrelserna som har ansvaret att tillse att GDPR följs.

Det är också förklaringen till varför det register som Rädda Barnen är skyldiga att föra enligt art 30 GDPR är uppbyggt efter vilka behandlingar som identifierats ute på våra avd/sektioner. Det finns en sorteringsfunktion utifrån de system behandlingarna anknyter till men den är sekundär.



Lokalföreningar respektive distrikt har tilldelats e-postadresser genom Office 365 där även lagrings- och bearbetningsmöjligheter finns för all föreningarnas respektive distriktens verksamhet. Office 365 är ett system som ligger under kansliet och därmed under ovan beskrivna riktlinjer

Varje lokalförening respektive distrikt är en egen juridisk person. Det är respektive styrelse som ansvarar för att de personuppgifter som förekommer i verksamheten behandlas korrekt. En förutsättning för att kunna uppfylla den skyldigheten är att styrelsen har kännedom om var och hur personuppgifter faktiskt behandlas. Varje lokalförening respektive distrikt behöver därför ha ett eget register över behandlingar.

Rädda Barnen har tillsatt en Dataskyddsansvarig som ska vara kontaktpunkt för alla personuppgifts-frågor både internt och externt samt vara stöd men även drivande i framtagande av nödvändiga riktlinjer och rutiner.

Grundläggande riktlinjer

Den personliga integriteten ska skyddas.

Se det som om vi lånar personernas information. De ska veta vad vi har och vad vi gör med den. De ska också kunna ta tillbaka den när de vill och då får vi inte längre använda den.

Användandet av personuppgifterna ska vara knutet till oss och vår verksamhet. Försäkra dig om att vi har en rättslig grund d v s att vi enligt GDPR har rätt att över huvud taget behandla personuppgifter för det ändamål/syfte du tänkt dig.

Personuppgifterna ska vara korrekta d v s rättstavade namn, rätt adress kopplad till rätt person, mejladresser som inte studsar.

Personuppgifterna ska skyddas mot förvanskning och radering d v s det är viktigt att det inte blir fel och kontroll är lättare att ha om inte för många personer har tillgång och back up-system måste finnas.

Personuppgifterna ska skyddas mot otillbörlig åtkomst d v s bara den eller de som ska komma åt uppgifterna ska göra det. Det gäller att ha inloggningsskydd och att fråga sig vem som behöver vilka uppgifter.

Dela dokument på samarbetsytor i stället för att skicka kopior av samma dokument fram och tillbaka.

Uppgiftsminimering gäller. Ta bara in nödvändiga personuppgifter. Fråga dig alltid om du behöver alla uppgifter. Behövs både namn, adress, telefonnummer och mejl vid en anmälan till en aktivitet eller utbildning? Fråga dig också om du behöver personuppgifter över huvud taget. Kan personen lika gärna vara anonym? I så fall gäller inte GDPR.

Lagringsminimering gäller. Spara inte längre än nödvändigt. Bokföringslagen har företräde framför GDPR. Krav från givare eller motsvarande kan tillmötesgås. Avidentifiera eller radera personuppgifter när de inte längre behövs. Avidentifiering innebär att vi kan spara övriga uppgifter för statistik och planering (förutsatt att vi angivit det som ett ändamål). Rensa inkorgen. Inget ska sparas där.

Utdrag ur belastningsregistret får enbart visas upp och en notering får göras i en lista att så skett. Ett utdrag får aldrig sparas.

Informera innan/i samband med att uppgifterna tas in. Informera om syftet t ex anmälan, deltagande, påverkan/opinionsbildning men informera också om, och i så fall, vad mer vi vill göra med

personuppgifterna. Informera alltid om vår fullständiga integritetspolicy, länka och/eller ha med ett exemplar att läsa.

Vi ska kunna visa att vi har gjort rätt. Se till att dokumentera. Följ de riktlinjer och rutiner som lämnas.

Rättslig grund

Behandlingen av personuppgifter ska vara laglig. Det innefattar att vi för varje behandling ska ha identifierat en rättslig grund som vi stödjer oss på. Rädda Barnen stödjer sig på följande rättsliga grunder:

Fullgörande av avtal		Det som t ex rent faktiskt krävs för att bli medlem, köpa en vara eller en tjänst eller få en projektansökan beviljad och bekräftad. Återrapporteringskrav för projekt eller extern finansiering hör också hit. Anställningsavtal och konsultavtal hör också hit.
Rättslig förpliktelse		Grundar sig i lag eller förordning men även i kollektivavtal. Vår skyldighet att lämna uppgifter till Skatteverket och fullgöra vår bokföringsskyldighet hör hit. Det gör också våra skyldigheter och rättigheter som baseras på kollektivavtal och arbetsrättslig lagstiftning. Hit hör även Centrums vårdverksamhet och de orosanmälningar som de är skyldiga att göra enligt lag.
Samtycke		När vi bett om, och individen uttryckligen sagt, att vi får behandla hens uppgifter och förstått vad det betyder. Samtycke behövs ofta när vi behandlar känsliga personuppgifter (uppgifter om t ex hälsa). Samtycke används ofta när det gäller bilder. Observera att när det gäller barn så är huvudregeln att vårdnadshavares samtycke behövs, dock att barn och ungdomar med stigande ålder har en ökad grad av självbestämmanderätt. Ett undantag från samtycke från vårdnadshavare finns. Det gäller rent förebyggande och rådgivande verksamhet som erbjuds direkt till barn, där bör samtycke från den som har föräldraansvaret inte krävas. Samtycket ska vara dokumenterat.
Uppfyllande av allmän uppgift		När vi gör en orosanmälan enligt socialtjänstlagen vid misstanke att ett barn far illa.

Berättigat intresse		Här ställs Rädda Barnens intresse mot individens intresse av skydd av sin personliga integritet. Det som vägs mot varandra är vårt intresse av att så effektivt som möjligt göra största möjliga skillnad för barn och individens intresse av att vi inte på något sätt missbrukar eller överutnyttjar de personuppgifter hen lämnat till oss. Om vi endast använder personuppgifter när de verkligen behövs och det för tydliga ändamål *och* individen *rimligen kan förvänta* sig att vi använder hens uppgifter på det sättet så har vi ett berättigat intresse. Enkelt uttryckt är berättigat intresse när det anses OK för oss att använda en individs uppgifter i vår strävan att göra världen bättre för barn och vårt intresse alltså kan anses väga tyngst. Berättigat intresse är den grund som vi oftast stöder oss på. Det kan gälla allt från marknadsföring till epost, deltagarförteckningar och nätverk.

Uppfyllande av allmän uppgift

För resonemang rörande valet av den rättsliga grunden uppfyllande av allmän uppgift för orosanmälningar, se **Rättslig grund – orosanmälningar**

Berättigat intresse

Varje gång vi ska behandla personuppgifter med stöd av grunden berättigat intresse ska en avvägning göras och dokumenteras. Dokumentationen sker lämpligtvis i det system där behandlingen sker (t ex i vårt givar- och medlemsregister). Rutin ska finnas för hur dokumentation ska göras.

Den rättsliga grunden kan också ha lagts fast genom en generell bedömning av hur vissa typer av dokument innehållandes personuppgifter ska hanteras eller för hur personuppgifter i epost-system hanteras. Först vid avvikelse från den fastlagda hanteringen krävs en ny individuell bedömning.

Epost, deltagarförteckning, protokoll, kontaktlistor, kontaktlistor politiker, nätverk, mejllistor är exempel där bedömningen av berättigat intresse genomförts på generell nivå.

Känsliga uppgifter

Undvik i den mån det går att behandla känsliga uppgifter. Vad som är känsliga personuppgifter är definierat i GDPR. Det är uppgifter som rör ras/etniskt ursprung, hälsa, sexualliv, politiska åsikter, religiös/filosofisk övertygelse och uppgift om medlemskap i fackförening.

Känsliga personuppgifter får behandlas med stöd av samtycke. Samtycke ska dokumenteras.

Även utan samtycke får känsliga uppgifter behandlas under vissa förutsättningar. Känsliga personuppgifter får behandlas när den registrerade på ett tydligt sätt offentliggjort dem. Det gäller t ex politiskt aktiva med förtroendeuppdrag.

Känsliga uppgifter får även behandlas om det är nödvändigt med hänvisning till fullgörandet av skyldigheter och rättigheter inom arbetsrätten och social trygghet och skydd. Här krävs stöd i lag eller kollektivavtal. Detsamma gäller för Centrums vårdverksamhet.

När känsliga uppgifter behandlas ska åtkomst och säkerhet särskilt beaktas.

Personnummer

Personnummer är inte per definition en känslig personuppgift men ska ändå behandlas med försiktighet. Personnummer få behandlas utan samtycke när det är klart motiverat med hänsyn till vikten av säker identifiering eller ändamålet med behandlingen.

Personnummer ska inte användas om det inte är nödvändigt.

Uppgifter om brott/misstanke om brott

Utdrag ur belastningsregistret får enbart visas upp och en notering får göras i en lista att så skett. Ett utdrag får aldrig sparas.

Uppgifter om brott/misstanke om brott kan förekomma, och får behandlas, inom ramen för våra trygghetssystem (Tryggare Tillsammans, Policy skydd mot sexuella övergrepp och sexuellt utnyttjande) samt i vårt antikorruptionsarbete. Detsamma gäller för policy för visselblåsning samt för visselblåsfunktionen. Stor restriktivitet är påkallad och rutin ska finnas för hur uppgifter ska hanteras i de fall rättslig grund för behandling saknas.

Risk- och konsekvensbedömning

När en ny typ av behandling, särskilt med användning av ny teknik, ska införas ska en risk- och konsekvensbedömning ske. Det som ska bedömas är den planerade behandlingens konsekvenser för de registrerade vars personuppgifter berörs utifrån deras integritet och det intrång behandlingen kan medföra. Målet är att skydda människors fri- och rättigheter och minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk.

Vid upphandling av nya eller gamla tjänster, uppstart av nya verksamheter och verksamhetsgrenar ska en risk- och konsekvensbedömning göras.

En risk- och konsekvensbedömning, utifrån förändrade förhållanden, ska göras inom ramen för ordinarie produktområdesplan

Dataskyddsansvarig lämnar råd och stöd.

Behandlingsregister för GDPR

På kansliet är vi skyldiga att föra ett register över våra personuppgiftsbehandlingar.

Det är respektive informationsägare, processägare och produktägare som ansvar att anmäla nya behandlingar till Dataskyddsansvarig.

Även behandlingar som upphör ska rapporteras till Dataskyddsansvarig.

En ny behandling kan exempelvis vara: ett projekt, en tjänst, framtagandet eller användandet av en app, plattform eller molntjänst. Vid ny behandling ska relevanta rutiner tas fram för t ex dokumentation, gallring, lagring och säkerhet.

Blankett finns för anmälan. (Se GDPR-siten på Intranätet Charlie.)

Lokalföreningar respektive distrikt ska alla ha ett eget register över de personuppgiftsbehandlingar som sker hos dem. Mall med instruktioner finns på medlemssidorna.

De registrerades rättigheter

Det är av största vikt att de registrerades rättigheter respekteras.

Vi ska lämna information om vilka personuppgifter vi samlar in, varför vi gör det och hur länge vi sparar dem. Vi ska vara så tydliga som möjligt och hänvisa till vår integritetspolicy.

Vi ska på begäran ta fram ett registerutdrag men även kopia på de personuppgifter vi har om en registrerad. Vi ska också kunna tillmötesgå en begäran om att bli raderad.

Eftersom våra system inte är sammankopplade och skyldigheten även omfattar epost och word/excel-filer var de än finns i organisationen, ställer det höga krav på efterlevnad av den rutin som gäller begäran om registerutdrag/radering. Vi har även en tidsfrist om en månad som ska iakttas. Läs Rutin för registerutdrag eller radering av personuppgift för mer information.

De registrerades rättigheter och vårt ansvar gäller även personuppgifter som finns ute i lokalföreningar och distrikt.

Om en registrerad vänder sig till en lokalförening respektive distrikt med en begäran om registerutdrag eller att bli raderad (eller annan rättighet) ska lokalförening respektive distrikt ta emot begäran och omedelbart kontakta Dataskyddsansvarig.

Personuppgiftsincident

Personuppgiftsincidenter ska rapporteras enligt gällande rutin.

Personuppgiftsincident är 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.

Epost

E-post innebär i princip alltid att man behandlar personuppgifter. Själva e-postadressen i sig är oftast en personuppgift och all annan information i meddelandet som kan kopplas till en enskild person är också personuppgifter.

I all vår e-post som vi skickar finns en kort information på svenska och engelska om att vi hanterar personuppgifter samt en hänvisning till vår integritetspolicy I vår integritetspolicy finns e-post omnämnt som en plats där vi får in personuppgifter. Ändamålet är att kunna upprätthålla en kontakt och utföra uppgifter.

E-post är nödvändigt för att effektivt kunna sköta vår verksamhet. Den rättsliga grunden för e-post är berättigat intresse.

När e-post tagits emot och lästs ska det bedömas om uppgifterna ska bevaras och var i så fall det ska ske.

E-posten ska rensas (städas) minst en gång om året.

Känsliga personuppgifter får normalt sett inte skickas med e-post.

Närmare precisering av hantering av personuppgifter i e-post ges i rutin Rutininsamling för personuppgiftsbehandling

Uppföljning

Uppföljning av efterlevnad av denna riktlinje kommer ske årligen, Dataskyddsansvarig initierar

uppföljning.

Revidering av denna riktlinje sker vartannat år.

Definition av begrepp

Term	Definition
Personuppgift	Personuppgift är alla uppgifter som direkt eller indirekt kan identifiera en fysisk, nu levande, person t ex namn, personnummer, telefonnummer, adress, fingeravtryck, foto, mejladress, kontonummer, IP-nummer och lokaliseringsuppgift (GPS-koordinater).
Behandling	Är i princip allt vi gör med en personuppgift t ex samlar in, lagrar, ändrar, raderar, skriver in, skickar vidare. Det spelar inte någon roll om det sker digitalt eller manuellt. Enda undantaget är dina handskrivna anteckningar som du aldrig avser sortera efter någon form av kriterier eller föra in i ett register. Så snart du renskriver dem i datorn blir det dock en behandling.
Avidentifiering	Att ta bort uppgifter så att en person inte längre kan identifieras. Resterande information i dokument, förteckning, system behålls. Statistik kan föras och planering av kommande verksamhet underlättas.
Registrerad	Den vars personuppgifter vi behandlar.
Känsliga personuppgifter	Personuppgift som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgift om hälsa eller sexuell läggning eller sexualliv samt genetiska uppgifter eller biometriska uppgifter.

Stödjande dokument

Dokument (t ex mallar) som stödjer policyn och dess genomförande:

- Informationssäkerhetspolicy med tillhörande instruktioner.
- Riktlinjer för samverkan i IT förvaltning
- Blankett personuppgiftsbehandling
- Mall register för lokalföringar respektive distrikt jämte instruktion
- Rutin för registerutdrag eller radering av personuppgifter
- Rutin för personuppgiftsincident
- Integritetspolicy
- Rättslig grund – orosanmälningar