Barns och ungas rättigheter på digitala plattformar

En vägledning till aktörer

BARN OMBUDS MANNEN

Datainspektionen

Statens medieråd

Bakom vägledningen står Datainspektionen, Barnombudsmannen och Statens medieråd.

FÖRORD

Skydda och stärk barns och ungas rättigheter

När barns och ungas vardagsliv i allt högre utsträckning utspelar sig i digitala miljöer är det av yttersta vikt att deras fri- och rättigheter tas tillvara där, precis som i den fysiska världen.

Barn och unga rör sig snabbt och vant mellan olika tjänster, men det är inte alltid synonymt med att de inser risker eller förstår konsekvenser – konsekvenser som dessutom kan ligga långt in i framtiden.

Att reglera internet är ofta svårt. Lagstiftningen är ibland komplicerad att tolka, språket är långt ifrån det språkbruk berörda själva använder och perspektiven är sällan så holistiska som de kan behöva vara när man betraktar en händelse ur ett barns perspektiv. Något vi kan sägas vara skyldiga att göra, sedan barnkonventionen blev lag i Sverige den 1 januari år 2020.

Det är därför vi, tre statliga myndigheter med särskilt ansvar för att skydda barn och unga och stärka deras rättigheter, valt att utifrån våra olika expertområden gemensamt ta fram denna vägledning.

Vägledningens syfte är att ge generellt stöd främst utifrån ett integritetsperspektiv (där dataskyddsförordningen, GDPR, är en central lagstiftning) och ett barnrättsperspektiv (utifrån barnkonventionen). Vägledningen innehåller också vissa råd baserade på lagstiftarens intentioner när det gäller att skydda barn från skadlig mediepåverkan.

Med vägledningen riktar vi oss primärt till aktörer som skapar och ansvarar för olika digitala miljöer där det är vanligt att barn och unga befinner sig. Oavsett om ni äger eller skapar webbplatser, svenskspråkiga plattformar eller har en egen Youtube-kanal hoppas vi att ni kommer att ha glädje av vägledningen.

Vi är övertygade om att vi tillsammans – när vi sätter barnens bästa främst – kommer att lyckas skapa trygga, säkra, digitala miljöer, anpassade efter barns och ungas behov.

Stockholm 2020

Datainspektionen
Barnombudsmannen
Statens medieråd

Innehåll

Förord 3

Kapitel 1: Introduktion 5

Trygga digitala miljöer för barn och unga 5
Barnets bästa – enligt barnkonventionen 6
Barnets rättigheter – enligt dataskyddsförordningen 7
Skydda barn från skadlig mediepåverkan 10
Checklista vägledningen i korthet 13

Kapitel 2 14

1 Vad krävs för att få behandla namn, bilder och andra personuppgifter 14
2 Möjlighet att ge samtycke 20
3 Riskbedömning 25
4 Krav på radering och information 29
5 Onlineverktyg 33
6 Spara och skydda personuppgifter 34
7 Ålderskontroll 35
8 Dela vidare personuppgifter 36
9 Använda personuppgifter i marknadsföringssyfte 38
10 Geo-lokaliseringsdata 39
11 Föräldrakontroll 40
12 Profilering 42
13 Nudging 43
14 Uppkopplade leksaker 44

Mer information och vägledning 47

Trygga digitala miljöer för barn och unga

Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter. Det är målet med regeringens digitaliseringsstrategi. Den digitala världen påverkar samhället på alla nivåer och som medborgare vänjer vi oss vid att det mesta går att göra digitalt, oavsett om det handlar om att kontakta myndigheter, göra ärenden eller uträtta arbetsuppgifter.

För barn och unga har digitaliseringen av skolan och tillgången till uppkopplade enheter stor påverkan på deras vardag. Även yngre barn ska enligt förskolans läroplan få tillgång till digitala verktyg. Efter skolan ägnar många barn och unga dagligen en stor del av sin fritid åt strömmande medier, spel och sociala plattformar.

Ur ett barnrättsperspektiv är det tydligt att digitaliseringen väcker behov av trygga och säkra digitala miljöer anpassade efter barn och unga. Regeringen har uppmärksammat behovet av så kallad digital trygghet genom förstärkt säkerhet och integritet inom ramen för digitaliseringsstrategin. I strategin påpekas att privata och offentliga aktörer behöver agera på ett ansvarsfullt sätt och att det krävs säkra digitala system som värnar den personliga integriteten. I praktiken innebär det att man vid utveckling och användning av digitala verktyg och tjänster behöver följa de regler som finns till skydd av barn och unga.

Förhoppningsvis kan denna vägledning underlätta för alla som skapar och ansvarar för olika digitala miljöer och vill bidra till att ge barn och unga trygga digitala miljöer. Den kan läsas som en sammanfattning av vad man har att tänka på enligt barnkonventionen, dataskyddsförordningen och barns rätt till skydd mot skadlig mediepåverkan.

Barnets bästa – enligt barnkonventionen

Sverige antog FN:s konvention om barnets rättigheter (barnkonventionen) redan 1990. Från och med den 1 januari 2020 är barnkonventionen även svensk lag. Detta innebär att rättigheterna i barnkonventionen kan tillämpas som svensk lag och att barn ses som rättighetsbärare och därmed får en starkare ställning juridiskt.

Barnkonvention innehåller universella bestämmelser som syftar till att stödja barnets behov gällande säkerhet, hälsa, välbefinnande, familjerelationer, fysiska, psykologiska och emotionella utveckling, identitet, yttrandefrihet och integritet för att bilda sina egna åsikter och rätt att få komma till tals. Barnombudsmannen är en statlig myndighet med uppdrag att företräda barns och ungas rättigheter och intressen utifrån barnkonventionen.

Som skapare av och ansvarig för en digital miljö är det viktigt att ha kunskap om barns rättigheter för att kunna säkerställa att barn är skyddade och kan utvecklas i den digitala miljön. Utifrån barnkonventionens 54 artiklar är artikel 3 en av de grundprinciper vi särskilt kommer att belysa i denna vägledning. Artikel 3 slår fast att barnets bästa ska beaktas vid alla åtgärder och beslut som rör barn. Barnkonventionen pekar uttryckligen ut vuxnas roll i att skydda och främja barnets bästa. Alla som skapar tjänster som riktar sig till barn och unga kan bidra genom att vid varje beslut som rör erbjudandet och dess utformning ha barnets bästa i fokus och barnkonventionen som utgångspunkt.

För att sätta barnet i fokus och ha ett barnrättsperspektiv behövs grundläggande kunskaper i barnkonventionen. De olika artiklarna hänger samman och ska ses som en helhet. Alla rättigheter är inte relevanta i alla frågor som berör barn, men för att säkerställa ett barnrättsperspektiv ska minst barnkonventionens fyra grundprinciper genomsyra frågan.

Läs mer

www.barnombudsmannen.se/barnombudsmannen/barnkonventionen/

www.barnombudsmannen.se/globalassets/dokument-for-nedladdning/publikationer/en-skrift-om-barnkonventionen-uppdat.pdf

Barnkonventionens grundprinciper

Artikel 2 – varje barn har samma rättigheter och lika värde.

Artikel 3 – barnets bästa ska beaktas vid alla beslut som rör barn.

Artikel 6 – varje barn har rätt till liv och utveckling.

Artikel 12 – varje barn har rätt att uttrycka sin mening och få den respekterad.

Förutom grundprinciperna finns ett antal bestämmelser som kan vara extra relevanta gällande barns och ungas rättigheter på nätet. I den här vägledningen är artiklarna om barns yttrande- och informationsfrihet (artikel 13) och rätten till privat- och familjeliv (artikel 16) samt artikel 17 om massmediernas roll särskilt relevanta, likaså artikel 19 (fysiskt eller psykiskt våld) och artikel 36 (skydd mot annat utnyttjande).

Barnets rättigheter – enligt dataskyddsförordningen

I den här vägledningen redogörs för utvalda delar av de krav som dataskyddsförordningen, eller General Data Protection Regulation (GDPR), ställer när barns och ungas personuppgifter behandlas för olika ändamål.

GDPR med reglerna om dataskydd har sin grund i EU:s stadga om de grundläggande rättigheterna. Reglerna hänger samman med individens rätt till respekt för sitt privat- och familjeliv, som gäller enligt Europakonventionen. Ett skydd för den personliga integriteten finns även i svensk grundlag; regeringsformen. Både GDPR och Europakonventionen gäller som lag i Sverige. Dataskyddsförordningen är direkt tillämplig som lag i Sverige och i hela EU. Svensk rätt får inte stå i strid med förordningen.

Dataskyddsreglerna gäller i hela EU och har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter. Det finns dataskyddsmyndigheter i varje EU-land som övervakar att reglerna följs. I Sverige är detta Datainspektionen (som från och med 1 januari 2021 heter Integritetsskyddsmyndigheten).

I dataskyddsförordningen lyfts barn särskilt fram och det sägs att barns personuppgifter förtjänar särskilt skydd, eftersom barn kan vara mindre medvetna om berörda risker, följder och skyddsåtgärder samt om sina rättigheter när det gäller behandling av personuppgifter.

Detta avspeglas bland annat i en särskild regel om barn som säger att barn över 16 år kan samtycka till att deras personuppgifter används för användning av informationssamhällets tjänster, såsom sociala medier eller chattprogram. Varje medlemsstat har haft möjlighet att sänka den utpekade åldern i denna bestämmelse och i Sverige har det bestämts att barn över 13 år får samtycka i dessa fall.

GDPR innehåller ett antal grundläggande principer som kan sägas vara kärnan i förordningen och som är viktiga att förstå och tillämpa. Principerna innebär bland annat att ni som har ansvar för hantering om uppgifter om barn:

- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål.
- inte får behandla fler personuppgifter än vad som behövs för ändamålen.
- har att se till att personuppgifterna är riktiga.

- har att radera personuppgifterna när de inte längre behövs.
- har att skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och att de inte förloras eller förstörs.
- behöver kunna visa att och hur ni lever upp till dataskyddsförordningen.

Begrepp dataskyddsförordningen

En förutsättning för att kunna tillämpa dataskyddsförordningen är att man förstår vad vissa centrala begrepp betyder, som exempelvis personuppgiftsansvarig, personuppgiftsbiträde och registrerad.

Personuppgiftsansvarig är den organisation (till exempel aktiebolag, stiftelse, förening eller myndighet) som bestämmer för vilka ändamål som uppgifterna ska behandlas och hur behandlingen ska gå till. Det är alltså inte chefen på en arbetsplats eller en anställd som är personuppgiftsansvarig. Även en fysisk person kan vara personuppgiftsansvarig, vilket till exempel är fallet för enskilda firmor. I vägledningen tilltalar vi företrädare för den personuppgiftsansvariga organisationen och säger ”ni ska tänka på” etcetera.

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges egen organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ. Exempelvis används ofta molntjänstföretag eller andra externa leverantörer av it-tjänster som personuppgiftsbiträde. Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvariga och avtal mellan parterna måste finnas.

Gemensamt personuppgiftsansvar är när fler aktörer tillsammans bestämmer och har ansvar över en och samma behandling. Då har de ett gemensamt personuppgiftsansvar.

Med **den registrerade** menas den person vars uppgifter behandlas.

Fler definitioner finns längre fram i vägledningen.

Skyldigheter och rättigheter

Dataskyddsförordningen innehåller både skyldigheter för dem som behandlar personuppgifter och rättigheter för de individer vars uppgifter behandlas. Till skyldigheterna hör att beakta de grundläggande principerna som redovisats ovan. Här följer några av de rättigheter som gäller både barn och vuxna:

- Rätten att veta vem som behandlar personuppgifter, för vad och varför?
- Rätten att få tillgång till de personuppgifter en organisation har, kostnadsfritt, och att få en kopia i ett tillgängligt format.
- Rätten att invända mot att en organisation behandlar personuppgifter utan att samtycke givits, om inte allmänintresset går före. Rätten att när som helst invända mot att få så kallad direktreklam, alltså reklam som går direkt till mottagaren.
- Rätten att få uppgifter korrigerade om de är felaktiga, ofullständiga eller oriktiga när de behandlas av en organisation.

- Rätten att få uppgifter borttagna, kallas också rätten att bli glömd. Rättigheten gäller om någons uppgifter inte längre behövs eller behandlas olagligt. Även andra rättigheter, som yttrandefrihet, måste skyddas. Därför kan man inte alltid få bort personuppgifter som exempelvis visas genom sökning via en sökmotor.
- Rätten att flytta uppgifter handlar om när individers uppgifter används av ett företag efter att samtycke givits eller ett avtal undertecknats. Då kan uppgifterna återlämnas eller överföras till ett annat företag på begäran av individen. Detta kallas för rätten till "dataportabilitet".
- Rätt att få information om personuppgifter förloras innebär att organisationen som innehar uppgifter måste informera Datainspektionen om personuppgiftsincidenter som innebär en risk för enskildas integritet. Om incidenten utgör en hög risk för en enskild måste individen också informeras personligen.

Kom ihåg!

Begreppen GDPR och dataskyddsförordningen används synonymt i vägledningen och det är samma regler som menas. När flera aktörer är involverade i exempelvis en tjänst eller plattform måste varje part ta ansvar för sin del enligt dataskyddsförordningen och andra tillämpliga regler. GDPR gäller inte i den mån det skulle inkräkta på rättigheter enligt yttrandefrihetsgrundlagen (YGL). Detta gör att reglerna oftast inte gäller för publicering av personuppgifter på internet i de fall det rör sig om databaser med utgivningsbevis och massmedieföretags automatiskt skyddade databaser.

Att tänka på!

Informationen i den här vägledningen baseras på GDPR, vars regler gäller i hela EU. Vägledningen gör inte anspråk på att redogöra för samtliga dataskyddsregler globalt. Vägledningen har hämtat inspiration i en lagstadgad uppförandekod från den brittiska dataskyddsmyndigheten ICO (Age appropriate design: a code of practice for online services). Den har dock inte samma status som den brittiska uppförandekoden utan ska läsas som sedvanlig myndighetsinformation om de regler som finns.

Skydda barn från skadlig mediepåverkan

Hur kan barn skyddas från skadlig mediepåverkan i digitala miljöer? Vad betyder skadlig mediepåverkan och vad har det att göra med utformningen av digitala tjänster?

Begreppet kan delas in i flera olika delområden, bland annat:

- skadligt medieinnehåll,
- skadligt kommunikativt handlande,
- skadlig interaktionsdesign och
- skadligt handhavande.

De tre första är särskilt viktiga att känna till för den som skapar och ansvarar för olika digitala tjänster.

Med skadligt medieinnehåll menas innehåll som kan leda till att barn drabbas av negativa konsekvenser. Det kan röra sig om våld, skräck och pornografi. Sådant innehåll kan medföra en upplevelse av stark rädsla eller obehag i stunden eller att barnet senare får svårt att sova, drömmer mardrömmar eller inte vågar göra saker det brukar göra. Men skadligt medieinnehåll kan också vara sådant som kräver upprepad exponering men påverkar barnet på längre sikt, som propaganda, reklam eller problematiska skönhetsideal.

”Skadligt medieinnehåll är innehåll som kan leda till att barn drabbas av negativa konsekvenser.”

Skadligt kommunikativt handlande inbegriper någon form av social interaktion. Exempel på detta är nätmobbning, hat, hot, virtuella våldtäkter eller hets mot folkgrupp. Det kan röra sig om handlingar som primärt riktas mot någon eller några med direkt fientliga avsikter eller handlingar som utförs utan att utövaren tänker på hur agerandet drabbar andra. I dag kan vem som helst som har tillgång till teknik publicera innehåll i form av bland annat text, bild och ljud. Många digitala tjänster innehåller forum för detta, exempelvis i form av chattfunktioner där användare kan interagera. Ett användargenererat medieinnehåll kan finnas kvar långt efter själva tillfället för publiceringen och det kan spridas till fler än vad som egentligen avsetts.

Även så kallade beroendefrågor eller problematisk användning av skärmar räknas till skadligt kommunikativt handlande.

Med skadlig interaktionsdesign avses en utformning av användarupplevelsen som leder barn och unga till val som kan vara skadliga för dem, som till exempel att lämna ifrån sig känsliga personuppgifter eller personliga bilder.

Skadligt handhavande ligger utanför fokus för vägledningen och rör negativa effekter av stillasittande och överdriven medieanvändning såsom övervikt, sömnproblem och förslitningsskador.

Hur skyddas barn?

Inom många områden i samhället har barn bedömts ha särskilda behov av skydd. Även deras rättigheter ska tillgodoses.

Att skydda barn från skadligt innehåll är ett sådant område, eftersom barn kan vara mindre kritiska och därför mer mottagliga för olika typer av budskap.

Åtgärder för att skydda barn från skadlig mediepåverkan – i lag och självreglering

Enligt marknadsföringslagen är det förbjudet att skicka direktreklam till barn under 16 år och att rikta direkta köpuppmaningar till minderåriga. I radio- och tv-lagen finns bestämmelser med begränsningar av innehåll med våldsskildringar och pornografiska bilder. Barnkonventionen innehåller skrivningar om bland annat barns rätt till en trygg uppväxt och rätt till yttrandefrihet.

Enligt dataskyddsreglerna ska barns (och andras) personuppgifter skyddas. Det finns även uppförandekoder för att exempelvis motverka hat på nätet och frivilligt överenskomna bestämmelser som omfattar branschaktörer, till exempel näringslivets etiska regler om särskild aktsamhet beträffande marknadskommunikation riktad till barn och unga.

Skydd mot skadligt medieinnehåll

Barn kan skyddas från skadligt medieinnehåll genom exempelvis de åldersgränser som Statens medieråd fastställer för film som visas offentligt och sändningstillstånden som reglerar när på dygnet vissa typer av innehåll får sändas via linjärsänd tv. Internet är inte reglerat på samma vis, men för alla som tillhandahåller tjänster där barn och unga kan komma i kontakt med skadligt medieinnehåll är det viktigt att beakta barnkonventionen och barns rättigheter.

Barn har särskilt behov av skydd

Barnkonventionen har betydelse för att motverka att barn tar del av skadligt innehåll. Enligt bestämmelserna har barn rätt till att söka, ta emot och sprida information och tankar av alla slag. Men barn har också rätt till skydd från information som kan vara skadlig för dem, liksom skydd mot intrång i privatlivet och sådant som kan skada barnets heder eller rykte. Barn har också rätt till särskilt skydd för sin integritet och sina personuppgifter, särskilt när det gäller riktad reklam eller insamling av data från tjänster som är specifikt riktade mot barn.

AV-direktivet (direktiv om audiovisuella medietjänster)

Är genomfört i Sverige främst genom radio-och tv-lagen, med regler om tv och beställ-tv. Bestämmelserna handlar bland annat om utformning av reklam, annonsmängd och placering av annonser, skydd av minderåriga och bestämmelser om innehåll som uppmanar till hat. Direktivet har nyligen justerats, vilket kräver ändringar i radio-och tv-lagen som är väsentliga för aktörer som ansvarar för digitala plattformar. Ett nytt kapitel om videodelningsplattformar införs i lagen. Där ställs krav på att en leverantör av en videodelningsplattform ska vidta lämpliga åtgärder: användargenererade videor, tv-program eller audiovisuella kommersiella meddelanden med ingående våldsskildringar av verklighetstrogen karaktär eller med pornografiska bilder ska inte tillhandahållas på ett sådant sätt att det finns en betydande risk för att barn kan se dessa, om det inte av särskilda skäl ändå är försvarligt. Leverantören ska även vidta åtgärder så att sådana videor, tv-program och meddelanden inte har ett innehåll som avses bland annat i brottsbalkens bestämmelser om olaga hot, uppvigling, hets mot folkgrupp, olaga våldsskildring och barnpornografibrott. De nya reglerna föreslås träda i kraft den 1 december 2020.

Olika mognadsgrad påverkar

När man tar ställning till vad som är skadligt innehåll tar man hänsyn till barns känslomässiga och intellektuella mognad, vilken utvecklas kontinuerligt. Ju äldre barn blir desto större blir deras förmåga att hantera och förhålla sig till situationer som de ställs inför. Även barns förmåga att bedöma risker och förstå konsekvenser av sitt handlande är något som utvecklas över tid. Yngre barn kan exempelvis sakna de redskap som krävs för att hantera ett skrämmande medieinnehåll eller förstå konsekvenserna av att publicera bilder eller lämna ut personuppgifter. Graden av skydd påverkas således av hur målgruppen ser ut och av barns olika åldrar och mognadsgrad.

”Barns risk för utsatthet är således också en faktor som behöver beaktas när man skapar digitala miljöer där barn befinner sig.”

Mer utsatta än andra

Vissa barn löper en större risk att drabbas av skadlig mediepåverkan. Barn med neuropsykiatriska funktionsnedsättningar (NPF) använder generellt medier mer än genomsnittet. De uppger också i högre grad att de har utsatts för hot, mobbning eller att någon varit elak mot dem på internet. Även barn med intellektuell funktionsnedsättning anger i högre grad att någon varit dum mot dem på internet. Barns risk för utsatthet är således också en faktor som behöver beaktas när man skapar digitala miljöer där barn befinner sig.

Exempel på myndigheter på området

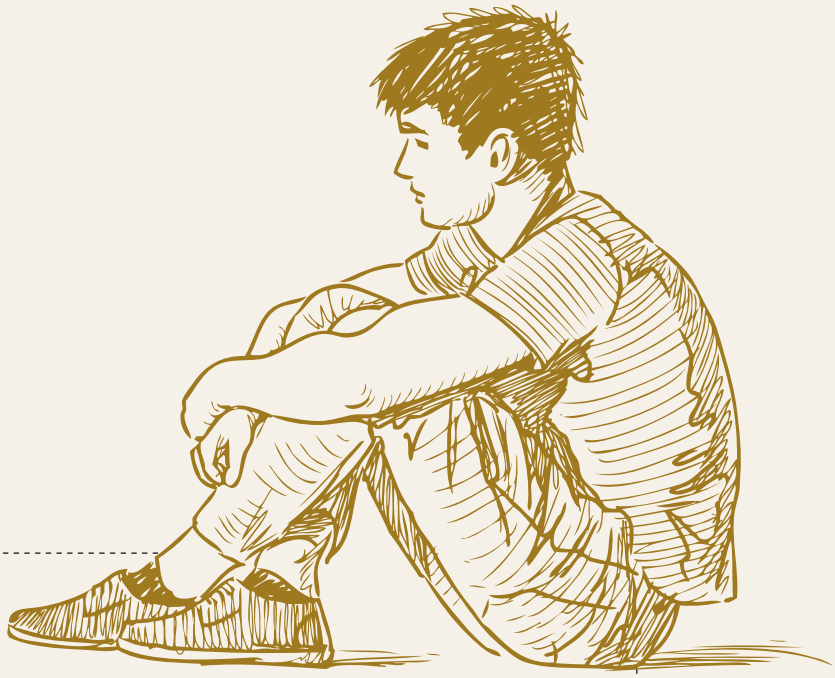
Statens medieråd

Konsumentverket

Myndigheten för press, radio och tv

Justitiekanslern

Polisen



Checklista – vägledningen i korthet

- Låt barnkonventionen och barnets bästa genomsyra er tjänst!
- Håll koll på viktiga begrepp! Personuppgift är inte bara namn och adress utan all information som kan kopplas till en person.
- För vilka syften behöver ni personuppgifter? Ändamålen bestämmer bland annat vilka uppgifter ni får samla in, hur länge de får sparas och om ni får dela vidare uppgifterna.
- Utan stöd i dataskyddsförordningen, GDPR, får ni inte använda personuppgifter! Samtycke och avtal är exempel på rättsliga grunder som kan göra det lagligt att hantera personuppgifter.
- GDPR-säkra era samtycken! Samtycke ska ske som en tydlig viljeyttring, utan påtryckningar med möjlighet att när som helst återkalla det.
- Ge information om hur uppgifterna om barn ska användas! Informationen ska vara barnanpassad när ni vänder er till barn.
- Gör en riskbedömning innan personuppgifterna samlas in! Det är ett lagkrav och hjälper er att planera de åtgärder ni måste vidta för att skydda personuppgifterna.
- Ha beredskap för att hantera enskildas rättigheter enligt dataskyddsförordningen, såsom begäran om registerutdrag och radering!
- Behandla så få personuppgifter som möjligt och ta hänsyn till integritetsaspekter och barnskydd vid planering och utformande av tjänster och system.
- Motverka hot och hat på era plattformar och skydda barn från skadlig mediepåverkan!

KAPITEL 2

1. Vad krävs för att få behandla namn, bilder och andra personuppgifter?

Samtycke krävs inte alltid – men är ibland nödvändigt

Ett vanligt missförstånd är att man alltid måste ha personers samtycke för att få publicera eller på annat sätt behandla deras personuppgifter. Så är det inte. Vad som däremot alltid behövs enligt dataskyddsförordningens regler är någon form av rättslig grund. Utan en rättslig grund är det nämligen förbjudet att behandla personuppgifter. Om ni vill behandla personuppgifter måste ni därför hitta en bestämmelse i förordningen (en rättslig grund) som passar som stöd för det ni ska göra, annars är behandlingen olaglig. Finns ingen annan rättslig grund som fungerar i sammanhanget kan samtycke vara det enda alternativet. Det krävs då att samtycket uppfyller en rad kriterier för att vara rättsligt giltigt, till exempel att det ska vara informerat och frivilligt och kunna återkallas. Här kan det vara värt att påminna om att barn inte alltid anses tillräckligt gamla för att få samtycka.

Läs mer om
hur den rättsliga grunden samtycke används på ett lagligt sätt i avsnitt två, sid 20. Där finns även information om vid vilken ålder barn kan börja fatta beslut om sina personuppgifter.

Personuppgift och personuppgiftsbehandling

Är all slags information som kan knytas till en levande person. Det kan röra sig om namn, adress och personnummer. Även foton på personer klassas som personuppgifter. Ja, till och med ljudinspelningar som lagras digitalt kan vara personuppgifter även om det inte nämns några namn i inspelningen. Ett bolagsnummer är oftast inte en personuppgift, om det inte handlar om ett enmansföretag. Registreringsnumret på en bil kan vara en personuppgift, om det går att knyta till en fysisk person. Personuppgiftsbehandling är allting man gör med personuppgifter: samlar in, sparar, delar, sorterar, publicerar och så vidare.

De rättsliga grunderna

Nedan nämns de rättsliga grunder som organisationer i privat verksamhet i första hand använder sig av.

Samtycke
Kan under vissa förutsättningar användas som rättslig grund för en personuppgiftsbehandling.

Avtal
Kan användas som rättslig grund för att behandla barns personuppgifter om det är nödvändigt för att fullgöra det man kommit överens om i ett avtal. Avtal kan bara användas om barnet är tillräckligt gammalt för att i det enskilda fallet själv kunna bestämma över sina personuppgifter.

Rättslig förpliktelse
Lagar eller regler gör att man ibland måste behandla vissa personuppgifter i sin verksamhet.

Intresseavvägning
Innebär att den personuppgiftsansvariga frågar sig om organisationens intressen väger tyngre än den enskilda personens och om behandlingen kan anses nödvändig för det aktuella ändamål som den ansvarige har. Om svaret är ja är behandlingen laglig med stöd av den rättsliga grunden intresseavvägning. Även inom offentlig verksamhet, som vid myndigheter, används avtal och rättslig förpliktelse som rättslig grund. För offentlig verksamhet kan även personuppgifter behandlas som ett led i ett allmänt intresse och myndighetsutövning (den vanligaste rättsliga grunden för offentlig verksamhet). Samtycke och intresseavvägning kan vanligen inte användas som rättslig grund i offentlig verksamhet.

Läs mer om
villkoren för samtycke, barns möjlighet att samtycka och om när minderåriga kan bestämma över sina personuppgifter i avsnitt två, sid 20.

Att tänka på – vid val av rättslig grund!

Varför behöver personuppgifterna behandlas? Ändamålen sätter ramarna för vad som är tillåtet och avgör vilken rättslig grund som är lämplig.

Dataskyddsförordningen ställer krav på att man specificerar ändamålen. Orsaken är att det inte är okej att samla in fler personuppgifter än vad som behövs för de konkreta ändamål som identifierats.

Det kan bli aktuellt att tillämpa olika rättsliga grunder för olika ändamål. Att använda personuppgifter för att leverera en vara till en kund och för att skicka reklam till kunden är exempel på två olika ändamål.

Oftast är samtycke varken det lättaste eller lämpligaste alternativet, bland annat för att den som givit sitt samtycke när som helst kan ta tillbaka det. Då måste personuppgiftsbehandlingen upphöra.

Finns ett avtal?

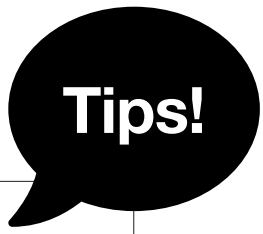
Samtycke behövs oftast inte när det finns ett avtal med en person. Vid exempelvis ett onlineköp förväntar sig kunden att få sin vara levererad. För att varan ska kunna levereras behöver butiken använda vissa personuppgifter, som kundens adress. De uppgifter som är nödvändiga för att kunna uppfylla avtalet får alltså behandlas med avtalet som rättslig grund. Om verksamheten vill använda personuppgifter för andra ändamål än för att uppfylla avtalet, till exempel för att skicka reklam, måste kunden ge sitt samtycke.

Intresseavvägning

Om ett avtal saknas och det är svårt att använda samtycke är det ofta möjligt att stödja sig på en intresseavvägning, vilket är den mest flexibla rättsliga grunden av alla. Då krävs att den tänkta personuppgiftsbehandlingen är nödvändig för ett ändamål som rör ett så kallat berättigat intresse, och att individens intresse av skydd för sina personuppgifter inte väger tyngre än det berättigade intresset hos verksamheten.

Vilka intressen hos en verksamhet är då berättigade? Exempelvis behandling av personuppgifter som är absolut nödvändig för att förhindra bedrägerier, men även behandling av personuppgifter för direktmarknadsföring anses vara ett berättigat intresse. Även om det finns ett berättigat intresse så måste ni bedöma om den tänkta personuppgiftsbehandlingen är nödvändig för att uppfylla det berättigade intresset. Bedömer ni att ni kan använda intresseavvägning behöver ni också försäkra er om att skyddet för integriteten inte väger tyngre i det enskilda fallet. Den bedömningen avgörs av vilken inverkan personuppgiftsbehandlingen har på den personliga integriteten. Sammanfattningsvis fungerar en intresseavvägning ofta när personerna, vars uppgifter man vill behandla, förväntar sig en viss personuppgiftsbehandling.

Att barn har behov av särskilt skydd är en viktig komponent att ta hänsyn till i intresseavvägningen. Kan ni visa att ni inom ramen för den planerade personuppgiftsbehandlingen kan skydda barnens personuppgifter, ge tillräcklig information och i övrigt värna barnens integritet så påverkar det möjligheten för er att lagligt använda deras personuppgifter med stöd av en intresseavvägning.



Vilket intresse väger tyngst?

För att avgöra vilket intresse som väger tyngst kan en barnkonsekvensanalys göras. Analysen ska visa vilka konsekvenser och effekter som kan uppstå för barn vid olika handlingsalternativ.

- Hur påverkas barn av olika handlingsalternativ?
- Vilka blir konsekvenserna för barn som befinner sig i utsatta situationer och där det finns stor risk att rättigheterna kränks eller där rättigheterna inte kan tillgodoses fullt ut?

Att tänka på!

- Barn är individer med olika förutsättningar.
- Ta hänsyn till ålder och mognad.
- Val av rättslig grund ska dokumenteras. Bland annat för att de personer vars uppgifter behandlas har rätt att få information om den rättsliga grunden.
- Den rättsliga grunden ska bestämmas innan personuppgifterna samlas in.

Internetpublicering

Om det som publiceras på internet innehåller personuppgifter krävs, som vid all personuppgiftsbehandling, en rättslig grund. I vissa fall är det självklart att samtycke krävs, exempelvis när det handlar om uppgifter rörande barn med skyddad identitet. Vilken rättlig grund som är lämplig vid internetpublicering avgörs av sammanhanget, som hur integritetskänsliga uppgifter det rör sig om. Är man osäker på hur man ska se på en publicering i dataskyddsförordningens mening är det alltid klokt att be om samtycke från berörda personer. Vid typiskt sett harmlösa publiceringar, i sammanhang med många berörda personer som exempelvis ett företags mingelbilder från ett event, kan det oftast vara mer lämpligt att stödja personuppgiftsbehandlingen på exempelvis en intresseavvägning. Tänk på att bilder och andra personuppgifter om barn alltid anses särskilt skyddsvärda. Barn kan ha svårare att förutse riskerna med att lämna ifrån sig uppgifter och förstå vilken rätt till skydd de har för sina uppgifter.

I vissa fall gäller inte dataskyddsförordningens regler för internetpubliceringar även om de innehåller personuppgifter. För grundlagsskyddade publiceringar är GDPR till stora delar inte tillämplig. Till exempel har en tidskrifts webbsida och även webbsändningar under vissa förutsättningar ett automatiskt grundlagsskydd. Exempel på grundlagsskyddade webbplatser är aftonbladet.se och dn.se. Andra vars databaser inte omfattas av ett automatiskt grundlagsskydd kan ansöka om ett utgivningsbevis som ger ett motsvarande grundlagsskydd för deras webbplatser. Exempel på webbplatser med grundlagsskydd genom utgivningsbevis är eniro.se och hitta.se.

Har ni en plattform som på grund av grundlagsskydd inte omfattas fullt ut av dataskyddsreglerna så finns andra regler som blir aktuella för er. Den som driver den grundlagsskyddade verksamheten är skyldig att utse och anmäla en ansvarig utgivare till Myndigheten för press, radio och tv. Utgivaren är juridiskt ansvarig om yttrandefrihetsbrott begås, till exempel hets mot folkgrupp, förtal eller förolämpning. Vidare ställer lagen om ansvar för elektroniska anslagstavlor krav på den som äger eller ansvarar för en sajt. Den som tillhandahåller tjänsten måste ta bort inlägg som innebär till exempel hets mot folkgrupp, uppvigling, olaga våldsskildring, barnpornografibrott och upphovsrättsintrång.

Vem ska ta ansvar för rättslig grund när flera aktörer är inblandade?

Vid alla typer av verksamheter (som tjänster och plattformar) där flera aktörer är inblandade är det viktigt att alla parter är medvetna om vilket ansvar de har för den behandling av personuppgifter som pågår. Flera parter kan bära ansvar samtidigt. I samma stund som ni har tillgång till personuppgifter måste ni ställa er frågan: Vilket ansvar har vi för uppgifterna? Det är viktigt att ni utreder om ni bär ansvar som personuppgiftsansvarig eller personuppgiftsbiträde. Vad dessa begrepp betyder förklarades i kapitel ett.

Som personuppgiftsansvarig verksamhet, tänk på dessa lagkrav:

- Ni har ansvar för att behandlingen sker i enlighet med dataskyddsförordningens samtliga bestämmelser.
- Ni kan överlåta den faktiska behandlingen av personuppgifter (till exempel hela det praktiska arbetet med en tjänst, hanteringen av ert kundregister och så vidare), men personuppgiftsansvaret kan aldrig lämnas över.
- Ni måste upprätta ett så kallat biträdesavtal mellan er och personuppgiftsbiträdet.

Har ni rollen som personuppgiftsbiträde, tänk på dessa lagkrav:

- Ni får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvariga och ni får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av den personuppgiftsansvariga.
- En del skyldigheter som ställs på personuppgiftsansvariga gäller även er, som att föra register över behandlingar, att säkerställa en lämplig säkerhetsnivå och att i vissa fall utse ett dataskyddsombud.

Både den personuppgiftsansvariga och personuppgiftsbiträdet kan bli föremål för tillsyn eller administrativa sanktionsavgifter och bli skadeståndsansvarig.

Den här vägledningen vänder sig i första hand till aktörer, med barn som målgrupp, men det kan vara bra att veta att även vårdnadshavare (och alla privatpersoner) har ett ansvar för personuppgifter som behandlas av dem. Behandlar man personuppgifter under en verksamhets ledning, som på jobbet, är det dock arbetsplatsen som är ansvarig eller biträde. Föräldrar till barn som är tillräckligt stora att själva bestämma över sina personuppgifter behöver kunna stödja sin personuppgiftsbehandling, av sitt barns (eller andras) personuppgifter, på en rättslig grund.

Tänk på att behandling av personuppgifter som träffas av det så kallade privatundantaget inte omfattas av GDPR. Det gäller behandling av personuppgifter som en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med dennes hushåll. Undantaget gäller dock inte när en privatperson offentliggör personuppgifter på ett sätt som gör uppgifterna tillgängliga för ett odefinierbart antal människor, till exempel genom öppen publicering på internet. Då måste man alltid följa dataskyddsförordningens regler.

Läs mer om
föräldrakontroll i avsnitt elva, sid 40.

Mer information

Råd om hur man gör en intresseavvägning och information om alla de rättsliga grunderna:

www.datainspektionen.se/lagar--regler/dataskyddsforordningen/rattslig-grund/intresseavvagning/

Vad innebär allmänt intresse och myndighetsutövning?

www.datainspektionen.se/lagar--regler/dataskyddsforordningen/rattslig-grund/myndighetsutovning-och-uppgifter-av-allmant-intresse/

Vad gäller när man använder den rättsliga grunden avtal för onlinetjänster – se vägledning från dataskyddsmyndigheternas samarbetsorgan:

www.datainspektionen.se/globalassets/dokument/eu/avtal-som-rattslig-grund-vid-anvandning-av-onlinetjanster.pdf

Så kan en barnkonsekvensanalys göras:

www.barnombudsmannen.se/barnombudsmannen/publikationer/genomfora-barnkonventionen/provning-av-barnets-basta/

Vad gäller vid personuppgiftsbehandling för offentlig verksamhet?

www.datainspektionen.se/

Åtgärder som Datainspektionen kan rikta mot den som bryter, eller riskerar att bryta mot reglerna:

www.datainspektionen.se/om-oss/arbetssatt/tillsyn/vad-kan-tillsynen-leda-till/

2. Möjlighet att ge samtycke

Kan barn och unga själva bestämma över sina personuppgifter?

Barn över 13 år kan enligt dataskyddsreglerna samtycka till att deras personuppgifter används vid användning av informationssamhällets tjänster.

Exempel på sådana tjänster är sociala medier, bloggar, internetforum, videodelningsplattformar, chattprogram, onlinespel, appar med spel eller annat innehåll.

Det finns ingen särskilt angiven åldersgräns för när ett barn kan samtycka till att personuppgifter behandlas i andra situationer, enligt GDPR.

Ålder och mognad påverkar

Hur kan man då tänka i andra situationer än de som gäller informationssamhällets tjänster? När det gäller barn under 13 år bör alltid vårdnadshavarens samtycke inhämtas. Föräldrarna har huvudansvar för barnets uppfostran och utveckling utifrån vad som bedöms vara barnets bästa. Barn över 16 år har generellt en viss rätt att agera självständigt i samhället och kan till exempel disponera sin egen arbetsinkomst. Någon som fyllt 16 år bör som regel också kunna ge ett giltigt samtycke till behandling av personuppgifter.

Men vad gäller då för barn mellan 13 och 16 år? Jo, då behöver det i varje situation bedömas om barnet i just det sammanhanget kan anses ha förmåga att förstå konsekvenserna av ett samtycke. Faktorer som har betydelse för bedömningen är till exempel hur pass känsliga personuppgifter som barnet ska lämna ifrån sig, hur länge de ska sparas, barnets ålder och mognad.

”Åldersgränsen blir en avvägning mellan rätten till delaktighet och risken att barnet far illa.”

Ni måste ta ställning till om barnet kan förutse de konsekvenser som behandling av personuppgifter kan medföra och om barnet kan förstå vad hen samtycker till.

Åldersgränsen blir en avvägning mellan rätten till delaktighet och risken att barnet far illa. Det är i förhållande till denna risk viktigt att se till den rätt som varje barn har. Barnet har rätt att få information anpassad till sin ålder och

mognad samt rätt att uttrycka sina åsikter och ha del i åtgärder och beslut som påverkar barnets liv.

Även om förmågan att ta till sig mer komplex information och förstå konsekvenserna av sitt handlande utvecklas kontinuerligt ju äldre barn blir, finns stora skillnader mellan olika individer. För att förstå konsekvenserna av att exempelvis lämna ut sina personuppgifter kan vissa barn behöva mer stöd än vad som är förväntat utifrån deras kronologiska ålder.

Detta gäller särskilt barn med särskilda behov, såsom barn med intellektuella funktionsnedsättningar.

Eftersom barns och ungas ålder har så pass stor betydelse för möjligheten att låta dem lämna samtycken som är lagliga kan det i vissa fall vara nödvändigt att göra ålderskontroller.

Gör barnanpassad information

Genom att anpassa informationen till mottagaren kan vi i högre grad säkerställa att informationen når ut. När informationen ska anpassas till barn är det viktigt att tänka på följande:

- Skriv i klarspråk.
- Inte för lång text.
- Om vårdnadshavare behöver lämna sitt samtycke ska det tidigt och tydligt i texten framgå att barnet som det angår har rätt till informationen.
- Barn har olika förutsättningar. Behöver informationen finnas på andra språk eller kunna läsas upp?

Ibland kan det vara svårt att veta om informationen är barnanpassad. Ett tips är att låta en referensgrupp av barn vara delaktiga i framtagandet av en text.

Läs mer om

ålderskontroll i avsnitt sju, sid 35.

Att tänka på!

- Oavsett om barn eller vuxna givit ett giltigt samtycke måste personuppgiftsbehandlingen leva upp till resten av reglerna i dataskyddsförordningen, som exempelvis rätten till information om hur uppgifterna behandlas och tillräcklig säkerhet kring uppgifterna.
- Vårdnadshavares samtycke krävs inte för förebyggande eller rådgivande tjänster som erbjuds direkt till barn. Skälet till detta är att barn ska kunna söka råd eller stöd utan att föräldrarna känner till det, till exempel hos Bris.
- Enligt barnkonventionen har varje barn rätt att uttrycka sin åsikt i beslut som rör dem. Barnets bästa ska beaktas och barnet bli tillfrågat innan någon annan ger samtycke till att lämna ut barnets personuppgifter.

Lagkrav på samtycket

Samtycket ska vara frivilligt

För att ett samtycke ska vara giltigt måste det lämnas helt frivilligt. Med detta menas att den som samtycker har ett genuint fritt val och kontroll över sina personuppgifter. Frivilligt samtycke kan förklaras med följande punkter:

- **Utan påtryckningar.** Den registrerade ska inte känna sig tvungen att samtycka. Samtycket är inte giltigt om någon utsatts för påverkan i samband med att det lämnades, exempelvis om man inom ramen för en kundklubb tvingas gå med på att samtycka till reklamutskick under påtryckningen att annars förlora bonuspoäng.
- **Med ångerrätt.** Den som samtycker ska ha rätt att dra tillbaka samtycket, vilket ska vara tydligt förklarat. Det ska vara lika lätt att lämna ett samtycke som att dra tillbaka det, annars kan det bli ogiltigt. Det är särskilt viktigt när det gäller unga personer. Om den som lämnat sitt samtycke inte kan eller får återkalla det utan att drabbas av negativa konsekvenser är samtycket inte frivilligt. Om ett samtycke återkallas måste den personuppgiftsansvariga sluta med den behandling som baserades på samtycket.
- **Jämlikt förhållande mellan den som behandlar och den vars uppgifter behandlas.** För att samtycket ska anses vara frivilligt måste förhållandet mellan den som behandlar personuppgifterna och den vars personuppgifter behandlas vara ”jämlikt” i dataskyddsreglernas mening. Exempelvis kan samtycke inte användas som en rättslig grund i förhållande till elever på en skola i undervisningen på grund av det ojämlika förhållandet mellan elever och skolan. Elever måste gå i skolan och får betyg där och kan därför inte känna att de frivilligt kan säga nej. Det är också anledningen till att samtycke som huvudregel inte kan användas som rättslig grund i offentliga verksamheter. Däremot kan samtycke användas utanför skolans ordinarie verksamhet, exempelvis vid skolfotografering.

”För att ett samtycke ska vara giltigt måste det lämnas helt frivilligt.”

Samtycke ska vara lämnat för varje ändamål för sig

Ett samtycke uppfyller inte kravet på frivillighet om ni bakar ihop flera syften. Om det finns flera olika ändamål till varför ni vill använda personuppgifter måste ni för att det ska anses frivilligt och giltigt ha samtycke till varje ändamål för sig. Om exempelvis ett företag vill fråga om samtycke för att dels få använda sina kunders uppgifter för att vända sig till dem med riktad reklam, dels ge kunderna möjlighet att delta i en särskild tävling, så är det olika ändamål. Att tvinga kunderna att tacka ja eller nej till ”allt eller inget” är inte lagligt.

Låt oss i detta sammanhang påminna om exemplet från avsnittet innan, om nätbutiken som kan behöva behandla personuppgifter för flera olika ändamål. Ni bör då överväga vilken rättslig grund som är lämplig för varje enskilt ändamål. Finns det personuppgifter som bedöms nödvändiga för att exempelvis kunna leverera varor?

Då bör personuppgiftsbehandlingen ingå i köpeavtalet med den registrerade. Ta inte med något i avtalet som kräver ett separat samtycke, utan låt avtalsvillkoren endast bestå av det som hör hemma där.

Ni får exempelvis inte villkora leverans av varor med att personen tvingas samtycka till att personuppgifter lämnas ut till annat företag, om det inte är nödvändigt för att köpeavtalet ska uppfyllas.

Samtycket måste vara specificerat

För att de unga som samtycker ska förstå vad de säger ja till måste beskrivningen av ändamålen vara detaljerad och anpassad efter deras ålder. Regeln har tillkommit för att skydda användarna från en hantering där den som ska behandla uppgifterna uttrycker sig otydligt i tron att senare kunna använda personuppgifterna i andra syften. Det är inte lagligt. Formuleringar som exempelvis att personuppgifterna ska användas i ”framtida kommersiella syften” är inte tillräckligt specificerade och ger inte ett lagligt samtycke.

Samtycket måste ge uttryck för en tydlig viljeyttring

Det får inte finnas några tvivel om att den som ska lämna sitt samtycke tydligt har godkänt hanteringen. Det krävs ett utlåtande eller en tydlig bekräftelse från den registrerade. Detta ska vara en medveten handling. Designen av gränssnittet måste därför innebära ett aktivt val, till exempel att kryssa i en ruta. Redan ikryssade rutor eller andra så kallade opt out-lösningar, det vill säga lösningar som kräver en aktiv handling från personen för att undkomma att samtycka, är inte lagligt. Samma sak gäller formuleringar där tysthet eller inaktivitet görs till ett aktivt val, som till exempel ”om du inte väljer något utgår vi från att du samtycker”.

Information krävs när samtycke inhämtas

När det gäller barn och unga måste ni vara extra vaksamma på att de verkligen har uppnått mognad att förstå och samtycka till behandlingen. Information som riktar sig till barn ska vara skriven på ett tydligt och enkelt sätt. Tänk på att minderåriga har olika förutsättningar. Vet ni inte hur gammal den ni kommunicerar med är? Designa så de allra yngsta förstår. En grundregel för alla aktörer som vill uppfylla barnkonventionens skrivningar om medbestämmanderätt är att utgå från att barnet måste ha förmåga att förstå vad det samtycker till. Vägs inte detta in kan ett lämnat samtycke vara ogiltigt. Det är den som samlar in uppgifterna som har att visa att samtycket är giltigt. För att en information ska anses tydlig nog behöver den innehålla följande punkter:

”Ni måste vara extra vaksamma på att barn och unga verkligen har uppnått mognad att förstå och samtycka.”

- Vem som begär samtycke, alltså vilka ni är.
- Vilken typ av personuppgifter ni tänker behandla.
- I vilket syfte ni vill använda personuppgifterna. Är det fler än ett syfte, beskriv vart och ett.
- Att det är möjligt att dra tillbaka sitt samtycke och hur.

Personuppgiftsansvarig måste kunna visa att giltigt samtycke inhämtats

Den personuppgiftsansvariga måste kunna visa att denne lever upp till reglerna. Den personuppgiftsansvariga har bevisbördan för att ett giltigt samtycke har inhämtats och för att den registrerade har fått relevant information. Därför är det nödvändigt att dokumentera hur och när samtycket inhämtades samt vilken information den registrerade fick.

Checklista för inhämtande av samtycke

Tänk på detta innan:

- Kontrollera att samtycke är den mest lämpliga lagliga grunden för behandling av personuppgifter.
- Säkerställ att begäran om samtycke framgår tydligt och är åtskilt från övriga villkor.
- Undvik att göra samtycke till en förutsättning för en tjänst.

Informera mottagaren om:

- Namn på den som är personuppgiftsansvarig för tjänsten.
- Namn på dataskyddsombudet, om det finns ett.
- Namn på eventuell tredje part, exempelvis en annan organisation som kommer få del av uppgifterna.
- Hur barnet drar tillbaka sitt samtycke.
- Att barnet kan vägra att samtycka utan att drabbas av negativa konsekvenser.

Tänk på när ni kommunicerar:

- Förklara varför ni vill ha uppgifterna och vad ni ska göra med dem.
- Använd inte förvalt samtycke, exempelvis genom förmarkerade rutor. Samtycke ska vara ett aktivt val.
- Använd ett tydligt och enkelt språk som är lätt att förstå.
- Var specifik och ge tydliga alternativ för olika ändamål, säkerställ separata medgivanden för separata personuppgiftsbehandlingar. Vagt eller allmänt samtycke är inte tillräckligt.

Skapa ordning och reda i rutinerna genom att:

- Dokumentera bevis för samtycket: vem, när, hur och vilken information som gavs.
- Granska kontinuerligt metoden för att inhämta samtycke och uppdatera den vid behov.
- Håll samtyckesförfrågningar separerade från övriga villkor

För att stå beredd om ett samtycke återkallas:

- Säkerställ att personuppgifter kan raderas omgående.

Läs mer

Vägledning från dataskyddsmyndigheternas samarbetsorgan:
www.datainspektionen.se/globalassets/dokument/riktlinjer-om-samtycke.pdf

3. Riskbedömning

Krav på att analysera risker inför behandling av personuppgifter

Ni måste alltid göra en riskbedömning innan ni påbörjar en behandling av personuppgifter. Detta gäller oavsett om ni exempelvis tänker lansera en ny app, en webbtjänst eller en egen kanal. Under hela den pågående personuppgiftsbehandlingen är ni också skyldiga att bedöma risker och i övrigt skydda och ta hand om uppgifterna på rätt sätt.

”Ni måste alltid göra en riskbedömning innan ni påbörjar en behandling av personuppgifter.”

Riskbedömningen avgör vilka åtgärder som krävs

Anledningen till att en riskbedömning ska göras är att den ger svar på vilka åtgärder ni behöver vidta för att skydda personuppgifterna i er specifika verksamhet. Ni måste genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa – och även kunna visa – att behandlingen utförs enligt dataskyddsreglerna. Åtgärderna som vidtas måste regelbundet ses över och uppdateras vid behov. Tekniska åtgärder är exempelvis åtgärder för kryptering eller autentisering. Organisatoriska åtgärder kan handla om noggranna rutiner för de personer som arbetar med uppgifterna, exempelvis att inte fler personer än nödvändigt tar del av uppgifterna.

Men hur vet man vad som är lämpliga åtgärder i det enskilda fallet? Det kräver att ni tar hänsyn till vilken typ av personuppgiftsbehandling det handlar om, personuppgifternas art, sammanhanget och tänkbara risker för uppgifterna i det enskilda fallet. Ni behöver fundera på hur sannolikt det är att en händelse inträffar som innebär risk för personuppgifterna och hur allvarliga konsekvenserna blir om händelsen inträffar.

Ett exempel på en risk kan det vara om det saknas tillräcklig säkerhet, så att “fel” personer får tillgång till personlig eller känslig information. Det kan handla om personuppgifter som kan leda till risk för diskriminering, identitetsstöld, bedrägeri, ekonomisk förlust eller skadat anseende. Desto högre sannolikhet för risk, desto högre säkerhet krävs.

Förutom risken för den enskildes personliga integritet bör ni i er riskbedömning beakta risken för att mänskliga rättigheter enligt Europakonventionen äventyras, som exempelvis yttrandefrihet, tankefrihet, fri rörlighet, förbud mot

diskriminering, rätt till frihet och religion. Även de särskilda rättigheter som barn och unga har enligt barnkonventionen ska omfattas av er riskanalys, bland annat att barn ska skyddas från alla former av våld och diskriminering och att principen om barnets bästa samt rätten för barn att komma till tals beaktas.

Konsekvensbedömning

Om riskbedömningen visar att er planerade personuppgiftsbehandling sannolikt leder till en hög risk för att enskilda personers fri- och rättigheter kränks krävs enligt GDPR en särskild så kallad konsekvensbedömning.

Konsekvensbedömning krävs enligt dataskyddsreglerna alltid i följande tre fall:

- Vid systematisk och omfattande bedömning av fysiska personers personliga aspekter, som grundar sig på automatisk behandling, inbegripet profilering.
- Vid behandling av känsliga personuppgifter i stor omfattning.
- Vid systematisk övervakning av en allmän plats i stor omfattning.

Läs mer om
profilering i avsnitt tolv, sid 42.

Vad detta innebär i praktiken är tydligare i Datainspektionens förteckning över när en konsekvensbedömning ska göras. Förteckningen är gjord med hjälp av riktlinjer och kriterier från den Europeiska dataskyddsstyrelsen (EDPB). Enligt förteckningen ska en konsekvensbedömning bland annat göras i följande fall:

- Ett företag använder kunders lokaliseringsuppgifter, som till exempel inhämtas via en mobilapp, i syfte att rikta marknadsföring till kunden eller planera sina marknadsföringsstrategier.
- Ett företag inhämtar uppgifter från sociala medier för att profilera fysiska personer och därefter rikta marknadsföring till vissa utvalda grupper. Tänk på att det enligt marknadsföringslagen är förbjudet att rikta marknadsföring till barn under 12 år.
- En sökmotor på internet samlar in uppgifter om enskilda som använder tjänsten för att skapa kundprofiler och rikta marknadsföring.

Om konsekvensbedömningen visar att riskerna inte kan begränsas tillräckligt och att det finns en fortsatt hög risk, krävs förhandssamråd med Datainspektionen innan behandlingen påbörjas. Sådant samråd kräver att ni dokumenterat er

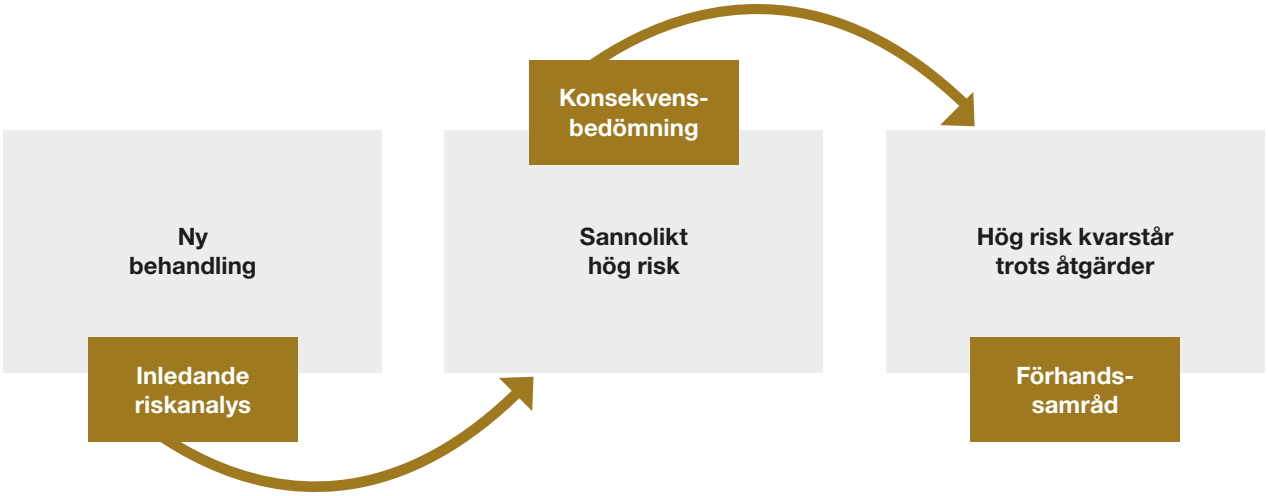
Europeiska dataskyddsstyrelsen,
European Data Protection Board, EDPB

Ett oberoende europeiskt organ som bidrar till att dataskyddsreglerna inom hela EU/EES tillämpas enhetligt. Främjar också samarbetet mellan dataskyddsmyndigheterna och ger allmän vägledning för att klargöra begrepp och tolka de rättigheter och skyldigheter som följer av reglerna i dataskyddsförordningen.

konsekvensbedömning och redogör för vilka risker som kvarstår och varför de inte kunnat åtgärdas.

Datainspektionen har möjlighet att förbjuda en behandling som strider mot dataskyddsförordningen. Som personuppgiftsansvarig eller personuppgiftsbiträde ska ni som huvudregel endast ha kontakt med ett lands tillsynsmyndighet, den så kallade "ansvariga tillsynsmyndigheten". För att veta vilken tillsynsmyndighet som är ansvarig måste ni ta reda på var er huvudsakliga eller enda del av verksamheten finns.

Riskbedömning enligt GDPR:



Läs mer om
hur en barnkonsekvensanalys kan göras i avsnitt två, sid 16.

Känsliga personuppgifter

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd. De kallas för känsliga personuppgifter.
Känsliga personuppgifter är uppgifter om:

- etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter
- biometriska uppgifter som används för att entydigt identifiera en person.

Det är som huvudregel förbjudet att behandla känsliga personuppgifter. Men det finns undantag; till exempel får ideella organisationer med politiskt, filosofiskt, religiöst eller fackligt syfte behandla känsliga personuppgifter om sina medlemmar. Det är också lagligt att behandla känsliga uppgifter om de registrerade uttryckligen har lämnat sitt samtycke.

Att tänka på!
Det finns många andra typer av personuppgifter som är särskilt skyddsvärda och som i praktiken kan kräva samma säkerhetsåtgärder som känsliga personuppgifter. Det kan till exempel vara:

- Ekonomisk information.
- Uppgifter om att någon har begått ett brott.
- Värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler.
- Information som rör någons privata sfär.
- Uppgifter om sociala förhållanden.

Personuppgiftsincident

Innebär en säkerhetsincident som kan medföra risker för människors friheter och rättigheter, såsom diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning, finansiell förlust, eller brott mot sekretess eller tystnadsplikt. En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har blivit förstörda eller kommit i orätta händer. Alla organisationer måste anmäla vissa typer av personuppgiftsincidenter till Datainspektionen inom 72 timmar efter det att överträdelsen har upptäckts.

4. Krav på radering och information

Hur kan barns och ungas rätt säkras vid personuppgiftsbehandling?

Anpassa information efter ålder

Alla, barn såväl som vuxna, har rätt att få information om vad som ska hända med deras personuppgifter. Att informera barn kräver många gånger extra eftertanke. Barn kan antas vara mindre medvetna om konsekvenser och risker. Att noga förklara de aktuella risker som gäller i en viss situation och de åtgärder som verksamheten har vidtagit kommer att hjälpa barn (och deras vårdnadshavare) att förstå konsekvenserna av att dela sin information och insikt i hur de kan skydda sina personuppgifter och sin integritet.

Ni ska ge kort och tydlig information som är anpassad efter barnets ålder. Finns det möjlighet bör ni vid sidan av skriftlig information även använda enklare diagram, illustrationer, grafik eller rörligt material som kan få barnen intresserade av informationen. Om verksamhetens målgrupp täcker ett brett åldersintervall kan en lösning vara att skapa olika versioner för olika åldrar. Om ni väljer att bara ha en version måste ni se till att den är tillgänglig för alla och kan förstås av de yngsta målgrupperna och de med intellektuell eller neuropsykiatrisk funktionsnedsättning.

I de fall då vårdnadshavares samtycke krävs för personuppgiftsbehandlingen, är det i första hand de som har rätt till information. Trots detta förlorar inte barnet sina rättigheter. I praktiken innebär det att ni ger både vårdnadshavare och barn tydlig och lättillgänglig information. Detta kan som sagt uppnås genom att utveckla olika versioner av information för olika målgrupper, eller genom att producera endast en barnvänlig version.

Krav på information

Informationen ska vara gratis, i en lättillgänglig form (vilken kan vara elektronisk) och med ett tydligt och enkelt språk. I dataskyddsförordningen anges utförligt vilken information som ska ges, bland annat ska den innehålla kontaktuppgifter till den personuppgiftsansvariga, den rättsliga grunden för behandlingen och ändamålet med behandlingen.

Information ska lämnas både när personuppgifterna samlas in och när den registrerade ber om den. Information måste även ges till de berörda, om det till exempel sker ett dataintrång eller liknande (en så kallad personuppgiftsincident) hos den personuppgiftsansvariga och det finns risk att personuppgifter läckt som skulle kunna leda till exempelvis identitetsstöld eller bedrägeri.

Barn som referensgrupp

När barnanpassad information ska tas fram kan det vara svårt att veta hur informationen upplevs av barn. Ett sätt att säkerställa att informationen upplevs korrekt är att ha med barn i en referensgrupp som får läsa igenom och lämna synpunkter på underlaget.

Hur når man barn?

- Ta kontakt med en skolklass, barn- och ungdomsorganisation etcetera.
- Använd er av en pop-up ruta på hemsidan med förfrågan om medverkan.
- Skicka ut en förfrågan i nyhetsbrev eller liknande.

Få inspiration till hur barnanpassad information kan se ut:
www.youmo.se/

Registerutdrag

Den registrerade har rätt att vända sig till er för att få veta vilka personuppgifter ni behandlar om individen och på vilket sätt. Ni ska då ge personen ett så kallat registerutdrag.

Registerutdraget ska innehålla information om vilka uppgifter som behandlas, var uppgifterna kommer från, ändamålet med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna lämnats ut. Registerutdraget ska normalt ges senast en månad efter att begäran inkommit.

Det kan finnas omständigheter som medför att all information i registerutdraget inte ska lämnas ut, exempelvis på grund av bestämmelser i annan lagstiftning (såsom sekretess) eller att ett utlämnande av informationen medför nackdelar för andra. Den personuppgiftsansvariga bör tydligt kunna förklara med vilket stöd den eventuellt nekar tillgång till personuppgifter.

Rätt till radering (”rätten att bli glömd”)

Både barn och vuxna har viss rätt att få sina personuppgifter raderade. Även i de fall då den ursprungliga insamlingen och behandlingen har varit laglig kan uppgifterna behöva raderas efter begäran från den som berörs.

När någon ber om att få sina uppgifter raderade måste ni tillmötesgå det i bland annat följande fall:

- Om uppgifterna inte längre behövs för de ändamål de samlades in för.
- Om behandlingen grundar sig på samtycke och den berörda återkallar samtycket.
- Om behandlingen sker för direktmarknadsföring och den berörda inte vill ha reklam.
- Om personuppgifterna har behandlats olagligt.
- Om radering krävs för att uppfylla en rättslig skyldighet.
- Om personuppgifterna avser minderåriga och samlats in i samband med att barnet skapar en profil i ett socialt nätverk.

Tips!

Motverka hot och hat

I behov av material för att motverka hot och hat? På uppdrag av regeringen driver Statens medieråd No Hate Speech Movement, en kampanj som bland annat genomförs i syfte att höja kunskapen om rasism och liknande former av fientlighet på internet bland barn och unga.

Informationsmaterial, pedagogiska verktyg och rapporter på området:
statensmedierad.se/nohate.1295.html

Att tänka på!

- Vårdnadshavare behöver inte involveras vid radering av uppgifter, om den som uppgifterna berör är gammal nog att ta beslutet. Radering ska göras om barnet önskar detta och har uppnått en lämplig ålder för att bestämma över sina uppgifter, även om det var vårdnadshavare som ursprungligen gav samtycket.
- Om barnet är gammalt nog att ge eget samtycke, bör ni inte acceptera en begäran om radering från en vårdnadshavare utan att ta hänsyn till barnets önskemål.
- Det ska normalt vara lika lätt för ett barn att ta bort sina uppgifter som att lämna dem. Gör det lätt för barn att förstå vad som gäller och visa hur de kan utöva rätten att bli glömd.
- Rätten att bli glömd gäller inte alltid. Det finns vissa tvingande skäl som gör att den personuppgiftsansvariga i vissa fall kan få behålla personuppgifterna, trots individens invändningar. Det kan exempelvis handla om att personuppgifter ska få behandlas på internet på grund av yttrandefrihetsskäl. En sökmotor som får en begäran om att en sökträff ska tas bort ska exempelvis göra en avvägning mellan å ena sidan personens rätt till skydd av sitt privatliv och å andra sidan internetanvändarnas rätt till information. Omständigheter som talar för att en sökträff ska tas bort är exempelvis om personen är minderårig eller var minderårig när uppgifterna publicerades. Att en sökträff leder till påhopp och otrevliga kommentarer innebär inte nödvändigtvis att den ska tas bort om det samtidigt tydligt framgår att det är fråga om någons personliga åsikter. Sammanhanget i stort spelar också roll. Uppgifter som publicerats på ett diskussionsforum har exempelvis inte samma trovärdighet i allmänhetens ögon som uppgifter som publicerats i en etablerad tidning.

Läs mer om

vid vilken ålder barn kan fatta beslut om sina personuppgifter i avsnitt två, sid 20.

Mer information

Vägledning från dataskyddsmyndigheternas samarbetsorgan

www.datainspektionen.se/globalassets/dokument/riktlinjer-om-oppenhet-och-information-till-registrerade.pdf

Vilken information ska ges i olika situationer?

www.datainspektionen.se/lagar--regler/dataskyddsforordningen/de-registrerades-rattigheter/#information

5. Onlineverktyg

Hur kan verktygen bli tydliga för barn och unga?

Med onlineverktyg menar vi i det här sammanhanget mekanismer för att hjälpa enskilda att utöva sina rättigheter enkelt när de är online.

Barn och unga har egna rättigheter som anses särskilt skyddsvärda. Alla som behandlar personuppgifter är därför skyldiga att underlätta särskilt för barn och unga som vill utöva sina rättigheter. Ett sätt att göra detta är att erbjuda onlineverktyg för att ladda ned, radera, begränsa eller rätta personuppgifter. Verktygen kan även användas för att ladda ner egna personuppgifter eller för att låta användarna lämna in klagomål.

Att tänka på!

- Gör det tydligt för barn och unga att onlineverktyg finns. Det kan göras genom tydliga ikoner och genom att framhäva verktygen i användargränssnittet. Precis som alltid när ni vänder er till barn och unga bör information ges på ett effektivt och kortfattat sätt.
- En tumregel är att informationen ska kunna förstås av en genomsnittsmedlem av den avsedda målgruppen. Det är särskilt viktigt med ett klart och tydligt språk i informationen där barnets mognad och ålder har tagits i beaktande.
- Tänk även på att barn i de yngre åldrarna och barn med olika typer av funktionsnedsättningar kan behöva och har rätt till information i ett format som är särskilt anpassat för dem.
- Alla uppskattar inte onlineverktyg och automatiserade processer. Ni behöver även hantera begäranden som kommer in på andra sätt, som via e-post och brev.

6. Spara och skydda personuppgifter

Minimum av uppgifter

Eftersom all insamling av uppgifter om barn och unga kan sägas vara integritetskänslig i viss mån är det av extra vikt att respektera grundprincipen om att samla in så få uppgifter som möjligt om gruppen. Principen som kallas för uppgiftsminimering innebär att ni aldrig ska behandla fler personuppgifter än vad som behövs och att de personuppgifter som behandlas ska vara tydligt kopplade till ändamålet, det vill säga höra till saken. Inför varje ny behandling av personuppgifter ska ni därför ta ställning till vilka personuppgifter ni behöver som ett minimum för att behandlingen ska kunna genomföras.

Designa för skydd

Att endast samla in det absolut nödvändigaste ställer krav på att anpassa den tjänst eller det system som används för att samla in personuppgifter. Detta kallas dataskydd som standard (privacy by default). För en webbplattform kan det till exempel handla om att designa gränssnittet så de förvalda inställningarna innebär att inte mer information än nödvändigt samlas in, delas ut eller visas. Redan vid utformningen av it-system och rutiner ska ni ta hänsyn till uppgiftsminimering och andra integritetsskyddsaspekter. Detta kallas inbyggt dataskydd (privacy by design) och innebär att ni måste integrera dataskydd i tid och införliva det i era arbetsmetoder. Ni måste därför utforma behandling, produkter och system med vetskapen om att barn anses särskilt skyddsvärda och att de ska kunna känna sig säkra när de använder tjänster på nätet och att deras rätt till integritet och privatliv respekteras.

Tips!

Skydda barn från att dela data på ett olämpligt sätt

Ställ in sekretessinställningar för appar med “inte dela” som standard.

Skapa en extra pop-up-ruta som varnar för konsekvenserna av ett val barnet är på väg att göra.

Designa avgörande beslut i flera steg, med fördröjning, för att ge betänketid.

Inkludera en tydlig, barnvänlig förklaring av den ökade funktionaliteten och dess risker när barnet aktiverar “delningsläge”.

Att tänka på!

Det är lättare att integrera en barnvänlig design i ett system eller produkt från början än att försöka lägga till den senare. Här kan en konsekvensbedömning användas som hjälpmedel för att enklare komma fram till hur systemet behöver vara utformat. Även för sådana personuppgiftsbehandlingar som medför en lägre risk är en konsekvensbedömning en bra hjälp för att upptäcka och sedan bedöma och mildra dataskyddsrisker för barnet.

Läs mer om

konsekvensbedömning i avsnitt tre, sid 26.

7. Ålderskontroll

När är det lämpligt att kontrollera ålder?

Beroende av sammanhanget kan det i vissa fall vara lagligt att utföra ålderskontroller.

Ett barns ålder kan exempelvis påverka om hen kan samtycka till en personuppgiftsbehandling. Åldern kan även ha betydelse för riskbedömningen. Därför kan det i vissa fall vara lämpligt eller nödvändigt för er att kontrollera ett barns ålder. Detta är bara lagligt när det finns ett tydligt behov. Utöver dataskyddsreglerna finns det i andra regelverk skyldigheter i förhållande till barn där ålderskontroll skulle kunna bli aktuellt. Exempelvis är leverantörer av videodelningsplattformar skyldiga att vidta lämpliga åtgärder så att innehåll som är skadligt för barn (till exempel våldsskildringar av verklighetstrogen karaktär eller med pornografiska bilder) inte tillhandahålls på ett sådant sätt att det finns en betydande risk för att barn kan ta del av det.

Det finns inga exakta regler om hur ålderskontroller ska göras, men de bör föregås av en riskbedömning och inte leda till orimlig behandling av personuppgifter. Mer ingående ålderskontroller kan i sig vara integritetskänsligt. Låt säga att det görs en riskbedömning och risken bedöms vara låg. Då kan det till exempel räcka med att be nya användare ange sitt födelseår eller fylla i ett formulär där de intygar att de inte är barn under en viss ålder. Ingående kontroller kan då genomföras om tvivel uppstår.

Läs mer om
riskbedömning i avsnitt tre, sid 25.

Finalitetsprincipen

Finalitetsprincipen innebär att personuppgifter vid ett senare tillfälle inte ska behandlas på ett sätt som är oförenligt med de ursprungliga ändamålen. Principen är tänkt att motverka att insamlade personuppgifter används på ett sätt som inte uppgavs vid insamlingen.

Mer information:

GDPR:s grundläggande principer

www.datainspektionen.se/lagar--regler/dataskyddsforordningen/grundlaggande-principer/

Att tänka på!

- Ta ställning till om det verkligen är nödvändigt med ålderskontroll.
- Samla in så få personuppgifter som möjligt.
- Använd inte personuppgifter som samlats in för ålderskontroll för andra syften, den så kallade finalitetsprincipen.
- Vid sidan om lagregler finns det inom vissa branscher självreglering som sätter åldersgränser som kan få betydelse för ålderskontroll. Ett exempel är PEGI, som är en europeisk standard för åldersrekommendationsmärkning av datorspel.

8. Dela vidare personuppgifter

Är det tillåtet?

Att dela vidare personuppgifter kan vara tillåtet såväl som otillåtet. Vad som gäller i ett specifikt fall beror på i vilket syfte som uppgifterna samlades in från början.

Utifrån vad som bedöms vara barnets bästa behövs en avvägning kring om delningen av barnets personuppgifter är lämplig. Hänsyn behöver tas till barnets rätt till delaktighet och information, liksom till barnets rätt att inte utsättas för ingrepp i sitt privatliv. Enligt dataskyddsreglerna är det ändamålet som avgör om ni kan dela vidare barns och ungas personuppgifter. Ni måste därför ha klart för er varför ni från början samlade in uppgifterna.

Är ändamålet att dela vidare uppgifter ett sådant ursprungligt ändamål, som ni har informerat de enskilda om, hittat en rättslig grund för och från början undersökt om det i övrigt uppfyller kraven i GDPR? Då är det troligt att delningen är tillåten.

Är ändamålet att dela vidare uppgifter ett nytt ändamål? Då kan delningen vara otillåten.

Är vidaredelningen av uppgifterna ett ursprungligt ändamål?

För det första måste ni alltså ha klart för er varför ni ska behandla personuppgifterna redan när ni börjar samla in dem. Ändamålen sätter nämligen ramarna för vad ni får och inte får göra, till exempel vilka uppgifter ni får behandla och hur länge ni får spara dem. Det är ändamålet som avgör om ni kan dela vidare barns och ungas personuppgifter.

Enligt dataskyddsförordningens princip om ändamålsbegränsning är det bara tillåtet att samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål. De registrerade har, som vi resonerat kring i tidigare avsnitt, rätt att få information om personuppgiftsbehandlingen. De måste bland annat få veta vilka mottagare som ska ta del av personuppgifterna.

Tillhör vidaredelningen av uppgifterna ett av era ursprungliga ändamål är den tillåten om ni, när behandlingen började, hade en rättslig grund och gav information till de registrerade.

Är det nya ändamålet förenligt med ursprungliga ändamål?

Om vidaredelningen är ett nytt ändamål ska ni ställa er följande fråga: Kan det nya ändamålet, att dela vidare uppgifter, sägas vara förenligt med de ursprungliga ändamålen? Är svaret ja kan ni stödja er på samma rättsliga grund som ni hade när ni samlade in personuppgifterna. För att komma fram till om det nya ändamålet är förenligt med tidigare ändamål är följande frågor till hjälp:

Vilken typ av personuppgifter ska ni behandla vid vidaredelningen? Är uppgifterna känsliga?

Vilken personuppgiftsbehandling kan de registrerade rimligen förvänta sig?

Vilka kopplingar finns mellan ändamålen med den ursprungliga personuppgiftsbehandlingen och den nya? Hur näraliggande är det nya ändamålet med de tidigare som de registrerade fått information om?

I vilket sammanhang har ni samlat in personuppgifterna? Vilket förhållande har de registrerade till er verksamhet?

Vilka konsekvenser kan personuppgiftsbehandlingen få för de registrerade?

Vilka skyddsåtgärder har ni, till exempel behörighetsstyrning, kryptering och pseudonymisering?

Läs mer om

hur en barnkonsekvensanalys kan göras – se avsnitt två, sid 16.

Vad gör vi om det nya ändamålet inte är förenligt med de ursprungliga ändamålen?

Om vidaredelning av personuppgifterna inte är förenligt med de ursprungliga ändamålen är det fråga om en helt ny personuppgiftsbehandling.

Ni måste då börja om från början och hitta en rättslig grund för personuppgiftsbehandlingen och stämma av så att den lever upp till övriga regler i GDPR.

Att tänka på!

- Vad som beskrivits ovan är förutsättningar för att lagligt lämna ifrån sig personuppgifter till en annan verksamhet. Den verksamhet som tar emot personuppgifter behöver också ha stöd för sin behandling i GDPR.
- Ni måste alltid lämna information om att uppgifterna ska delas vidare till den minderåriga eller dess vårdnadshavare (beroende på om barnet kan sägas ha åldern inne att själv bestämma om personuppgiftsbehandlingen).
- Det kan vara svårare för barn att fullt ut förutse konsekvenserna av att ens personuppgifter delas vidare. Därför är det extra viktigt att skydda barns personuppgifter och personliga integritet.
- Det ställs högre krav på enkel och lättförståelig information när man vänder sig till minderåriga.

9. Använda personuppgifter i marknadsföringssyfte

Är det lagligt?

Under vissa förutsättningar är det lagligt att använda personuppgifter i marknadsföringssyfte. Mot detta finns inget absolut förbud, men ni måste vara säkra på att ni lever upp till gällande regler på området. Om ni vill använda barns och ungas personuppgifter för marknadsföring måste ni alltid utgå från vad som bedöms vara barnets bästa.

Att använda minderårigas personuppgifter för marknadsföringsändamål kan exempelvis handla om att skicka reklam via e-post (direktreklam) eller att rikta anpassade annonser till barn och unga på plattformar som de besöker. Marknadsföring på internet förekommer i många olika former, exempelvis som banners, reklaminslag på videodelningsplattformar eller i spel eller annat som barn ofta använder. Det förekommer även marknadsföring inbäddad i sociala medier.

Innan ni använder barns och ungas personuppgifter i marknadsföringssyfte ska ni enligt GDPR:

- Göra en konsekvensbedömning.
- Hitta en rättslig grund.

Den rättsliga grund som ofta blir aktuell vid personuppgiftsbehandling för marknadsföring är intresseavvägning.

Barn är mindre medvetna om risker men förtjänar samtidigt ett särskilt skydd enligt reglerna. Därför är det i en intresseavvägning viktigt att beakta och skydda barnen mot risker som de kanske inte själva kan bedöma och konsekvenser som de själva inte är medvetna om. Detta gäller särskilt vid användningen av barns personuppgifter i marknadsföringssyfte, för att skapa användarprofiler och i tjänster som riktar sig direkt till barn.

Läs mer om

intresseavvägning i avsnitt ett, sid 15.

Mer information

www.konsumentverket.se/for-foretag/marknadsforing/marknadsforingslagen

Att tänka på!

- Barn har samma rätt som vuxna att när som helst invända mot direktreklam. Om ni tar emot en sådan invändning måste ni upphöra med utskicken. Att denna rättighet finns måste ni informera om i det första utskicket till de minderåriga eller innan ni börjar behandla personuppgifterna. Det måste finnas utarbetade rutiner för att upphöra med den typen av utskick.
- Utöver dataskyddsreglerna och barnkonventionen finns andra regler att ha koll på för den som vill rikta marknadsföring till barn och unga. Konsumentverket har tagit fram en användbar vägledning om vad som gäller enligt marknadsföringslagen för reklam riktad till barn och unga. Det är inte heller enligt dessa regler förbjudet att rikta marknadsföring på internet till barn, men det finns vissa regler att förhålla sig till:
  • Det är förbjudet enligt marknadsföringslagen att rikta direktreklam till barn under 16 år.
  • Ett barn ska förstå vad som är reklam och vad som inte är det. Därför får inte reklam utformas som spel, lekar eller liknande. Reklam får inte heller bakas in i spel på internet så att barn inte förstår vad som är reklam i spelet.

10. Geo-lokaliseringsdata

Får data användas som berättar var barn och unga befinner sig?

Vad som är barnets bästa kan variera i den enskilda situationen, men som huvudregel ska data som berättar var barn och unga befinner sig inte användas.

Geolokaliseringsdata (platsdata) är uppgifter om till exempel en mobiltelefons eller surfplattas geografiska position vid en viss tidpunkt. Platsdata kan göra det möjligt att dra ingående slutsatser om privatlivet för de personer som uppgifterna kan kopplas till, såsom deras vanor, var de bor, platser de besöker, rörelsemönster, aktiviteter och sociala relationer.

Platsdata ses som mycket integritetskänsliga. Generellt ökar riskerna för integritetsintrång med mängden av uppgifter och graden av precision, eftersom det möjliggör en mer ingående kartläggning av personen. Även enstaka uppgifter, exempelvis den exakta plats där ett barn för tillfället befinner sig, kan vara känsliga i dataskyddsreglernas mening. Om en uppgift exempelvis handlar om regelbundna besök på en klinik går det att dra slutsatser om hälsa, information som är att betrakta som känslig och kräver särskilt lagstöd.

Vid sidan om dataskyddsperspektivet innebär möjligheten att spåra ett barns plats en risk för att uppgifterna missbrukas i syfte att äventyra barns fysiska säkerhet. En varaktig delning av platsen kan också innebära att barns känsla av eget utrymme inskränks, vilket äventyrar barns och ungas rättigheter. Rätten till privatliv innebär att barn inte får kontrolleras eller utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv.

Att tänka på!

- När det gäller barn och unga bör grundinställningen vara att platsdata inte behandlas, om det inte finns tvingande skäl att göra det och barnets bästa har beaktats. Liksom för all personuppgiftsbehandling kräver användning av platsdata stöd i dataskyddsförordningens alla regler.
- Gör en konsekvensbedömning, överväg rättslig grund, säkerställ tillräcklig säkerhet för uppgifterna och ge information till de registrerade.
- Gör barn och unga medvetna om när platsdata samlas in, exempelvis genom att visa tydliga symboler. Tekniken i sig kan göra det svårt för minderåriga användare att förstå när personuppgifter samlas in och vilka konsekvenser det kan få.
- Lagra inte uppgifter längre än nödvändigt och använd i möjligaste mån metoder för att avidentifiera personuppgifterna.
- Vid sidan av dataskyddsreglerna finns i lagen om elektronisk kommunikation särskilda regler om lokaliseringsuppgifter från appar och mobilnät. Detta är Post- och telestyrelsen (PTS) tillsynsmyndighet över.

Mer information

Post- och telestyrelsen
pts.se/

11. Föräldrakontroll

Med verktyg för föräldrakontroll menas olika digitala lösningar som ger föräldrar eller vårdnadshavare möjligheten att begränsa eller kontrollera vad barn och unga kan göra på internet. Det kan handla om begränsningar av tillgång till internet men också vilka tjänster eller appar som kan användas, vilka webbplatser som kan besökas eller beloppsbegränsningar för köp i appar. Det kan också vara verktyg för att övervaka vad barn och unga gör på internet eller var de befinner sig.

Vårdnadshavare ska ta hänsyn till barnets önskemål

Enligt barnkonventionen ska barns rätt till privatliv respekteras. Verktyg för föräldrakontroll får därför bara användas om barnet har möjlighet att förstå att det övervakas och hur.

Barn ska inte kontrolleras eller utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv. Som vårdnadshavare har man huvudansvaret för barnets uppfostran och utveckling utifrån vad som bedöms vara barnets bästa. Föräldrar har här en svår balansgång att följa, som det gäller att vara medveten om. Enligt både föräldrabalken och barnkonventionen är föräldrarna skyldiga att skydda sina barn. De har även en stor bestämmanderätt över barnet. Vårdnadshavare ska i takt med barnets stigande ålder och utveckling ta allt större hänsyn till barnets synpunkter och önskemål. Ju äldre barnet är, desto mer hänsyn ska tas till barnets vilja och medbestämmande. Detta ska vårdnadshavare som använder verktyg för så kallad föräldrakontroll ta hänsyn till. Föräldrarna måste därför prata med sina barn, berätta vad olika verktyg är till för och ta in barnets åsikt innan ett verktyg börjar användas. Här måste också föräldern bland annat ta hänsyn till barnets rätt till privatliv, för att göra en avvägning av vilka verktyg som ska användas, hur och när. Det är viktigt att vårdnadshavare gör en nyanserad bedömning innan ett verktyg används, och pratar med barnet om verktyget, bland annat om varför det ska används.

För- och nackdelar med föräldrakontroll

Verktygen är viktiga eftersom de kan användas för att stödja vuxna när det gäller att skydda och främja barnets bästa. Men sådan övervakning kan också ha negativ påverkan på barns och ungas fri- och rättigheter. Det kan begränsa deras möjlighet till privatliv, lek, föreningsfrihet och tillgång till information och yttrandefrihet, vilket i sin tur kan påverka utvecklingen av deras egen identitet.

Verktygen kan även riskera att invagga vårdnadshavare i falsk trygghet. Vad gäller exempelvis innehållsfilter är det mycket svårt, kanske till och med omöjligt, att utveckla teknik som filtrerar precis lagom mycket. I praktiken tar filtren bort antingen för lite eller för mycket, vilket skapar olika typer av problem. Ett filter som tar bort för lite innehåll kan få vårdnadshavaren att släppa på sin vaksamhet och tro att filterlösningen har gjort internet till en säker zon för barnet. I själva verket filtreras inte allting bort och barnet kan vara exponerat för oönskat innehåll.

Ett filter som tar bort för mycket innehåll är också problematiskt. Låt säga att användaren tror sig ha installerat ett filter som till exempel stoppar pornografi, där verktyget i realiteten förhindrar åtkomsten till seriösa sexualupplysningssajter. Överblockering har visat sig slå hårdast mot dem som har svårast att hitta information offline, som exempelvis unga hbtq-personer.

Barn och unga kan också runda filtren genom att koppla upp sig hos vänner eller i andra sammanhang där vårdnadshavarnas regler inte gäller.

Information om utmaningarna med innehållsfilter kan med fördel ges till användarna. Den metod som rekommenderas är att tala med barnen, som annars riskerar att bli lämnade ensamma med sina upplevelser.

Informera barnet

Om ni erbjuder verktyg för föräldrakontroll bör ni tillhandahålla åldersanpassad information till barnet om detta. Det kan exempelvis vara symboler eller ikoner som visar för barnet när sådan spårning sker.

Värdefullt i sammanhanget är även information till föräldrar om barnets rätt till privatliv. I övrigt gäller att som vid all användning av tjänster och verktyg vari personuppgifter behandlas, att följa reglerna i GDPR om rättslig grund, säkerhet, riskbedömning, information med mera.

Läs mer om

parters ansvar enligt dataskyddsreglerna i kapitel ett, sid 7.

Att tänka på!

- Alla bär ansvar för sin egen hantering av personuppgifter, både tillhandahållare av ett verktyg för föräldrakontroll, vårdnadshavare eller andra användare.
- Om ni tillhandahåller innehållsfilter så kan ni med fördel informera era användare om riskerna med att använda ett sådant verktyg.

12. Profilering

Får barns och ungas personuppgifter användas för kategorisering av individer?

Både barn och vuxna har rätt att inte träffas av beslut som enbart grundas på automatiserat beslutsfattande där profilering varit en del av processen. Detta gäller om beslutet kan få stark påverkan på individen.

Vad gäller övrig profilering som inte handlar om automatiserat beslutsfattande sägs inget särskilt i GDPR. När ni vill använda profilering avseende barn måste ni fortfarande beakta alla regler, precis som vid all personuppgiftsbehandling. Bedömningen av vilken rättslig grund som är aktuell för en profilering beror som alltid på ändamålen. Om profileringen är nödvändig för en tjänst kan man eventuellt stödja sig på avtalet om tjänsten som rättslig grund. Profilering med enda syfte att skydda barn skulle stödja sig på den rättsliga grunden intresseavvägning, utifrån vad som kan antas vara barnets bästa. Ofta krävs samtycke vid profilering, eftersom profilering anses mycket integritetskänsligt och i de flesta situationer är svårt att försvara i förhållande till både barnkonventionen och dataskyddsreglerna.

Vad menas med profilering?

Innebär varje form av automatisk behandling av personuppgifter då en mängd uppgifter sammanställs och analyseras i syfte att bedöma vissa personliga egenskaper, i synnerhet för att analysera eller förutsäga bland annat personens hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

Om cookies/kakor

Många webbplatser skapar små filer med information om sina besökare och lagrar dem i besökarnas webbläsare. Dessa kallas webbkakor (engelska: ”cookies”) och behövs ofta för profilering. Som huvudregel krävs samtycke för att använda webbkakor. Detta regleras i lagen om elektronisk kommunikation (LEK), som Post- och telestyrelsen (PTS) är tillsynsmyndighet över.

Mer information

Post- och telestyrelsen
pts.se/

13. Nudging

Är det tillåtet att påverka barns och ungas val med hjälp av design?

Digital ”nudging” brukar användas för att beskriva hur en webbplats kan styra användarnas val genom hur upplevelsen designats. Genom att ge användarna en knuff (engelska: ”nudge”) i en viss riktning är det möjligt att närmast obemärkt styra deras beteende. Beroende på i vilket syfte designtekniken används är det tillåtet att påverka barns och ungas val med hjälp av design. Det kan vara fråga om otillåten nudging om barnet i praktiken inte har, eller endast har begränsade möjligheter, att relativt enkelt kunna göra väl avvägda val.

I en valsituation med alternativen ja och nej till viss personuppgiftsbehandling kan nudging exempelvis utövas genom att ja-alternativet visas som en stor grön knapp och nej-alternativet med en liten, otydlig text. Ett annat exempel är att förenkla ett visst val genom att erbjuda ett klick för det ena valet men en komplicerad process med många klick för det andra.

När nudging används stick i stäv med reglerna

GDPR förbjuder inte nudging, men det går i allmänhet emot principen om korrekthet och öppenhet i dataskyddsreglerna. Barn och unga har rätt till anpassad information utifrån ålder och mognad för att kunna fatta ett informerat beslut. Det är viktigt att motverka processer som är missvisande för barn.

Att använda nudging i en process som syftar till att inhämta ett samtycke till viss behandling kan exempelvis innebära att samtycket anses ogiltigt. Genom att använda nudging riskerar vi att äventyra kraven på att samtycke ska vara informerat och ske genom en otvetydig viljeyttring.

Nudging kan även vara problematiskt vid användning av förinställda åldersalternativ. Detta kan leda till att barn och unga lämnar fel uppgift om sin ålder. Det är därför inte att rekommendera.

Läs mer om
samtycke och vid vilken ålder barn kan samtycka i avsnitt två, sid 20.

Att tänka på!
Det är ofta inte designtekniken i sig som är problemet, utan hur den används. Nudging kan till exempel användas på sätt som ligger helt i linje med dataskyddsprinciperna och barns och ungas rättigheter, för att styra användare till det alternativ som ger starkast integritetsskydd.

Principen om korrekthet och öppenhet
Innebär enligt GDPR bland annat att personuppgiftsbehandlingen ska vara förståelig och begriplig för de registrerade och inte ske på dolda eller manipulerande sätt. Informationen om behandlingen ska vara lätt att hitta och formulerad på ett sätt som är enkelt och begripligt.

14. Uppkopplade leksaker

Vad gäller för anordningar som samlar in data?

Redan innan ett föremål köps och installeras ska det vara lätt att förstå att föremålet är uppkopplat mot internet och på vilket sätt det samlar in personuppgifter. När det gäller leksaker är det extra viktigt att informationen är enkel och tydlig. Lek och leksaker är ett område som traditionellt sett inte förknippas med insamling av personuppgifter. Tvärtom innebär leken ofta ett utforskande och experimenterande där barnet kan pröva olika idéer, roller och infall i en trygg miljö. Det blir därför extra viktigt att information om datainsamling i dessa sammanhang presenteras på ett sätt som är enkelt för barnet att förstå.

Exempel på uppkopplade leksaker och anordningar (internet of things)

Med uppkopplade leksaker och anordningar menas fysiska produkter som stöds av funktioner som tillhandahålls genom en digital uppkoppling.

- Det kan exempelvis handla om kramdjur som barnet kan prata med, där det barnet säger spelas in. Informationen i form av ljudklipp överförs till servrar, analyseras maskinellt och genererar instruktioner för anpassade svar som skickas tillbaka och spelas upp. Barnet kan uppfatta det som ett samtal med sitt kramdjur och därmed lockas att dela med sig av potentiellt integritetskänsliga uppgifter.
- Ett annat exempel är aktivitets- eller hälsoarmband som kontinuerligt registrerar potentiellt integritetskänsliga uppgifter om barnets fysiska aktivitet och överför uppgifterna till servrar där de sammanställs, lagras och används för att visas som aktivitetsrapporter i en app.
- Ytterligare ett exempel är så kallade röstassistenter installerade i användares hem. Dessa högtalare fångar upp röstkommandon och kan kommunicera information från internet till användaren, som att läsa upp nyheter och väder, boka tjänster eller beställa produkter. Högtalarna kan samla in en mängd uppgifter som användarna inte hade för avsikt att dela. Om högtalarna blir en del av medievardagen kan medvetenheten om den pågående informationsinsamlingen minska.

Genomtänkt information till användarna

Det är avgörande att leverantörer av dessa uppkopplade produkter och tjänster säkerställer att barn, unga och vårdnadshavare får den information de har rätt till. Det är viktigt att fundera kring hur uppkopplade apparater fungerar och vid vilka tillfällen det är lämpligast att kommunicera viss information till barnet eller vårdnadshavaren.

Information vid köptillfället

Tydlig information om att produkten behandlar personuppgifter ska ges till användarna vid köptillfället och innan produkten installeras. Detta kan göras både på den fysiska produktens förpackning och i bruksanvisningen, exempelvis med en ikon som visar att produkten är uppkopplad och behandlar användarnas personuppgifter. Potentiella köpare bör kunna ta del av integritetspolicy, användarvillkor och annan relevant och anpassad information online utan att först behöva köpa och installera produkten.

Information vid installation

Vid installationsprocessen av den uppkopplade leksaken eller produkten ges ett bra tillfälle att informera om hur tjänsten fungerar, hur personuppgifter används och konsekvenserna därav, särskilt om installationen görs med hjälp av ett skärmbaserat gränssnitt. Detta är särskilt viktigt om barnets fortsatta användning av produkten inte är skärmbaserad, eftersom det kan begränsa möjligheterna att fortlöpande överföra information till barnet.

Vem ansvarar för vad?

Olika aktörer kan bidra med olika delar i tillhandahållandet av ett uppkopplat föremål. Därför är det som tidigare nämnts viktigt att reda ut frågan om vem som är personuppgiftsansvarig eller personuppgiftsbiträde och för vilka delar av personuppgiftsbehandlingen som varje part ansvarar.

Vilka skyldigheter ni har varierar beroende på vilka roller ni har. Om ni som aktör anlitar ett annat företag (ett personuppgiftsbiträde) för att bistå med tjänsten har ni som personuppgiftsansvarig ett övergripande ansvar. I detta fall gäller bland annat att se till att även biträdet följer reglerna. Produkten måste ha lämpliga säkerhetsåtgärder för att minska risker som till exempel obehörig åtkomst till uppgifterna eller att produkten hackas för att spåra var barnet befinner sig.

Läs mer om
personuppgiftsansvarig och personuppgiftsbiträde på sid 8.

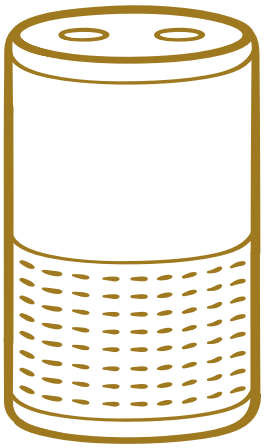
Mer information

www.barnombudsmannen.se/barnombudsmannen/barnkonventionen/

www.barnombudsmannen.se/globalassets/dokument-for-nedladdning/publikationer/en-skrift-om-barnkonventionen-uppdat.pdf

Att tänka på vid utformning av uppkopplade saker!

- Gör standardinställningarna integritetsvänliga.
- Undvik passiv insamling av personuppgifter och gör det tydligt när apparaten samlar in personuppgifter. Exempelvis kan en lampa tändas när apparaten spelar in ljud och bild eller samlar in personuppgifter på annat sätt.
- Det bör vara enkelt att slå av insamlingsläget på anordningen, exempelvis direkt på anordningen med en ”uppkoppling av”-knapp eller via funktioner online. Leksaken eller anordningen bör kunna användas utan uppkoppling i den utsträckning det är praktiskt möjligt.
- En uppkopplad anordning kan komma att användas samtidigt av användare i olika åldrar. Detta gäller särskilt smarta högtalare och röstassistenter avsedda att placeras i hemmet, vilka kan komma att behandla personuppgifter om flertalet hushållsmedlemmar och besökare. Uppkopplade leksaker kan användas av många, genom att de lånas ut eller används av flera barn som leker tillsammans. Tjänster och produkter bör därför anpassas för användning av alla dessa målgrupper. Vad gäller smarta högtalare kan det vara lämpligt att möjliggöra skapandet av olika användarprofiler, vilka kan anpassas utifrån användarnas ålder.



Tips!

Gör en referensgrupp

Gör gärna en referensgrupp av barn vid utformandet av en leksak. Då kan ni få reda på om målgruppen barn verkligen förstår när uppgifter inhämtas och när de inte gör det.

Mer information och vägledning

Barnombudsmannen

www.barnombudsmannen.se/barnombudsmannen/barnkonventionen/konventionstexten/

www.barnombudsmannen.se/globalassets/dokument-for-nedladdning/publikationer/allmanna-kommentarer/ak-20-svenska-formaterad.pdf

www.barnombudsmannen.se/globalassets/dokument-for-nedladdning/ak14_2019.pdf

Bris

www.bris.se/for-vuxna-om-barn/vanliga-amnen/unga-och-internet/barnets-vardag-pa-natet/

Europarådet

rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

www.coe.int/en/web/children/-/for-children-by-children-learn-about-your-rights-in-thedigital-environment-

Friends

www.dropbox.com/sh/w9pd82tqelkb4o2/AACIWnFZTp5-UXa3FYitEb0ha?dl=0&preview=Friends_natrapport_2017.pdf

Rädda Barnen

www.raddabarnen.se/rad-och-kunskap/foralder/skydda-ditt-barn-fran-att-raka-illa-ut-pa-natet/

Surfa lugnt

surfalugnt.se/

The EU Code of Conduct

ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

Detta är en vägledning från

BARN OMBUDS MANNEN

Datainspektionen

Statens medieråd