GDPR – Dataskyddsförordningen

Alla myndigheter, företag och föreningar måste kunna hantera personuppgifter för att kunna utföra uppdrag, service och tjänster. Samtidigt finns behov av regler för att skydda vår integritet och det finns därför bestämmelser om hur personuppgifter får hanteras.

Den 25 maj 2018 trädde EU:s Dataskyddsförordning/GDPR (eng. förkortning av General Data Protection Regulation) i kraft. Samma dag upphävdes personuppgiftslagen (PUL). Eftersom GDPR är en förordning är den direkt tillämplig som lag i Sverige. Den omfattar all behandling av personuppgifter som sker i myndigheter, föreningar och företag inom EU. Syftet är att ge medborgarna starkare rättigheter med fokus på ett ökat integritetsskydd.

Jämfört med tidigare PUL ställer GDPR strängare krav på hur personuppgifter samlas in och används. Den som bryter mot reglerna riskerar kännbara böter. Därför är det viktigt att känna till vad som gäller.

Vi förbundsjurister är inte specialister inom just detta område, men samlar i detta dokument viktig information om vad man behöver tänka på vid behandling av personuppgifter som rör barn, elever och deras föräldrar i förskolor och skolor. Det är Integritetsskyddsmyndigheten (IMY), tidigare Datainspektionen, som är ansvarig för frågor om persondataskydd och som kan ge vägledning i hur skolorna ska arbeta. Vi länkar sist i vår pm till deras hemsida, men även till annan information där man kan läsa mer.

Det kan också vara bra att som ingång i läsningen känna till att det för merparten av nödvändiga behandlingar av personuppgifter i förskola och skola kommer att finnas ett stöd i lagstiftningen samt att samtycke som grund för behandling bara ska kunna användas i undantagsfall.

Lite mer om dataskyddslagstiftningen för förskolor och skolor

GDPR är en EU-gemensam lagstiftning, men ger dock ett visst utrymme för medlemsländerna att i vissa delar ha kompletterande nationella bestämmelser där det behövs. Därför finns det dels en svensk dataskyddslag, dels inom utbildningsområdet ett särskilt 26 a kapitel i skollagen där man bedömt att det fanns behov av ytterligare kompletteringar för Sverige. I skollagskapitlet finns t.ex. regler om fristående huvudmäns möjligheter att behandla känsliga personuppgifter. Förarbetena till skollagens bestämmelser finns i proposition Behandling av personuppgifter på utbildningsområdet (prop. 2017/18:218).

Några av de viktigaste nyheterna med GDPR

Även om det nu har gått några år sedan GDPR började gälla som lag i Sverige, finns det anledning att lyfta fram några av de viktigaste nyheterna, här är de kortfattat och nedan går vi in lite närmare på de olika frågorna.

- Personuppgiftsansvarig är skyldig att kunna visa att GDPR följs och det ställs större krav på att arbeta systematiskt med dataskydd. Man behöver därför ha koll på vilka uppgifter som förs och varför.
- Krav på att ha en registerförteckning över de olika sätt som personuppgifter hanteras och av vem.
- Strängare krav på att informera berörda om hur deras personuppgifter hanteras.
- Förbud mot att behandla känsliga personuppgifter, om inte vissa förutsättningar gäller. Exempel på undantag är samtycke, inom hälso- och sjukvård, arbetsrätt eller kollektivavtal). I skollagen kommer det också att ges visst utrymme för sådan behandling.
- Den tidigare s.k. missbruksregeln i PUL försvann, dvs. undantaget som har möjliggjort personuppgiftsbehandling i löpande text (mejl, Word-filer, enkla listor). All sådan behandling måste alltså följa GDPRs regler. Det finns dock några bestämmelser som ger stöd för nödvändig behandling i ärenden m.m. enligt nedan.
- Högre krav på utformningen av samtycke.
- Skyldighet att rapportera förlorad kontroll av personuppgifter.
- Integritetsskyddsmyndigheten (IMY), som tidigare hette Datainspektionen, får större befogenheter.
- Nya och tuffare sanktioner infördes. Om man brister i sin behandling av personuppgifter kan man åläggas att betala en administrativ sanktionsavgift på upp till 20 miljoner euro eller fyra procent av organisationens omsättning.

Viktiga begrepp

En ***personuppgift*** är all slags information som kan knytas till en levande person, t.ex. namn, personnummer, e-postadress, uppgifter om hälsa och allergier, fotografier, betyg, IP-adress, nicknames med mera. Det är därför inte någon idé att börja kalla barn eller elever för förkortningar eller kodord för att komma undan bestämmelserna i GDPR – även sådana ”namn” går att knyta till en viss person.

Vissa personuppgifter är mer integritetsnära till sin natur och kategoriseras som ***känsliga personuppgifter*** och avser uppgifter om hälsa, etniskt ursprung, sexualliv och sexuell läggning, religion, politisk åskådning, genetiska och biometriska uppgifter för att identifiera en person samt fackligt medlemskap. De har ett starkare skydd i GDPR.

Med ***behandling*** av personuppgifter menas i princip allt som går att göra med uppgifterna, dvs. alla olika åtgärder eller kombinationer av åtgärder. Det kan t.ex. vara samla in, registrera, organisera, strukturera, lagra, bearbeta, lämna ut uppgifterna, med mera.

Personuppgiftsansvarig är den som är ytterst ansvarig för personuppgiftsbehandlingen (ofta ett företag eller organisation). För fristående förskolor och skolor är det företaget/organisationen, dvs. huvudmannen som är godkänd att bedriva förskolan/skolan. Huvudmannen företräds i sin tur av styrelsen.

Dataskyddsombud är den person som av personuppgiftsansvarig utsetts till att självständigt se till att personuppgifter behandlas på ett korrekt och lagligt sätt enligt GDPR. Dataskyddsombudet är också ombud för de registrerade. Myndigheter är skyldiga att ha ett ombud, men företag och organisationer får bedöma om det finns skäl för att utse ett sådant, t ex. om man hanterar stora mängder känsliga personuppgifter som en del i verksamheten. Utses ett ombud ska den personuppgiftsansvarige anmäla detta till IMY. På myndighetens webb finns mer information och rekommendationer att ta del av.

Personuppgiftsbiträde är den som *utanför* den personuppgiftsansvariges organisation behandlar personuppgifter för den personuppgiftsansvariges räkning. Det kan exempelvis vara olika systemleverantörer eller en leverantör av digitala läromedel. Om man vill anlita ett personuppgiftsbiträde måste ett skriftligt avtal tecknas. Avtalet ska bland annat innehålla instruktioner för hur biträdet får behandla personuppgifterna.

Personuppgiftsincidenter handlar om att man har utsatts för ett dataintrång eller råkat ut händelse där man förlorat kontrollen av personuppgifter som vid förlust av dator, USB-minne, telefon eller har råkat skicka vidare personuppgifter till någon obehörig, exempelvis ett mail med integritetskänsliga personuppgifter har skickats till fel person. Sådana incidenter måste i vissa fall rapporteras till IMY.

Grundläggande krav och principer för behandling av personuppgifter

Man måste ha stöd i dataskyddsförordningen för att få hantera personuppgifter, det måste finnas en rättslig grund för annars är behandlingen inte laglig (art 6.1 GDPR).

För att kunna behandla personuppgifter krävs att två saker är uppfyllda:

1. Att det finns en *rättslig grund* för behandlingen OCH
2. Att det finns ett *nödvändigt syfte/ändamål* med behandlingen.

Begreppet *rättslig grund* redogörs närmare för i nästa avsnitt.
Ändamålskravet innebär att man bara får samla in uppgifterna för särskilda, uttryckligen angivna och berättigade syften. Syftet/ändamålet måste man vara klar över *innan* insamlingen av personuppgifter börjar och uppgifterna får sedan inte behandlas på ett sätt som inte rimmar med syftet. Ändamålen ska dokumenteras skriftligt och den registrerade ska få information om det både när uppgifterna samlas in och annars när denne begär det.

Förutom kraven ovan finns ett antal grundläggande principer som måste beaktas:

1. Uppgifterna måste vara riktiga och uppdaterade (korrekta).
2. Uppgiftsminimering, dvs. uppgifterna ska vara adekvata, relevanta och man ska inte samla in fler personuppgifter än vad som är nödvändigt för det angivna ändamålet.
3. Uppgifterna får inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålen (lagringsminimering).
4. Behandlingen ske på ett tryggt och säkert sätt (integritet och konfidentialitet).
5. Behandlingen ska också ske med öppenhet för alla berörda (informationskrav).

Rättslig grund för behandling av personuppgifter

GDPR innehåller flera olika rättsliga grunder som innebär att verksamheten har rätt att behandla personuppgifter (tillsammans med ett tydligt ändamål). Rättslig grund kan utgöras av exempelvis allmänt intresse, rättslig förpliktelse (lag, beslut, kollektivavtal), myndighetsutövning, samtycke eller s.k. intresseavvägning. Ibland kan flera rättsliga grunder vara tillämpliga samtidigt. Som ovan nämndes kommer det att finnas stöd för behandling av i princip alla nödvändiga personuppgifter i förskolor och skolor. Samtycke från vårdnadshavare och elever kommer bara att behövas för vissa uppgifter och behandling.

Allmänt intresse (Art 6.1 e)

Begreppet allmänt intresse är ett unionsrättsligt begrepp som inte definieras någonstans, men man kan beskriva det som något som är av intresse för eller berör många människor på ett bredare plan. Man kan läsa mer om detta i regeringens prop. 2017/18:218 sid 42-47.

Att tillhandahålla utbildning och undervisning utifrån nationella krav och mål samt att tillhandahålla elevhälsa med allt vad detta innebär av personuppgiftsbehandling anses vara en uppgift av *allmänt intresse,* både när kommuner och friskolor utför den. Därtill finns många bestämmelser med utpekat ansvar för huvudmän, rektorer och

förskolechefer och lärare/förskollärare. Det finns därför behov av att kunna behandla personuppgifter för att kunna fullgöra uppgifter utifrån vad skollagstiftningen kräver.

I skollagstiftningen (skollagen, läroplanerna och skolformsförordningarna och skolmyndigheternas förskrifter) finns tydliga skrivningar om förskolans och skolans uppdrag och bestämmelser med många olika krav på vad verksamheterna är skyldiga att göra för att fullgöra kraven i förhållande till barn/elever och vårdnadshavare, beslut som ska fattas och dokumentation som ska finnas osv.

Allmänt intresse kommer därför att vara den vanligaste rättsliga grunden för många av de behandlingar som är nödvändiga att göra i era verksamheter. Men även andra rättsliga grunder kan samtidigt vara tillämpliga.

Rättslig förpliktelse (Art 6.1 c)

Det finns lagar eller regler som gör att den personuppgiftsansvarige måste behandla vissa personuppgifter i sin verksamhet. I skollagstiftningen finns det en hel del förpliktelser med ett tydligt syfte. Det handlar t.ex. om att eleven och vårdnadshavare fortlöpande ska informeras om elevens utveckling, att åtgärdsprogram ska utarbetas, att elever ska ges betyg, att modersmålsundervisning ska erbjudas i vissa fall m.m. Även orosanmälningar till socialtjänsten eller tillbudsrapporter till Arbetsmiljöverket är skyldigheter enligt lag. Dessa personuppgiftsbehandlingar utförs utifrån en rättslig förpliktelse.

Men som ovan nämndes kommer den rättsliga grunden allmänt intresse också att vara tillämplig i merparten av fallen.

Myndighetsutövning (Art 6.1 e)

Det handlar om att den personuppgiftsansvarige måste behandla personuppgifter för att utföra sina myndighetsuppgifter. Friskolor är visserligen inte myndigheter, men vissa uppgifter betraktas som myndighetsutövning. Typexemplet är betygssättning, men det finns också andra bestämmelser som handlar om ärendehandläggning i förskolor och skolor och om olika beslut som ska fattas, t.ex. mottagande av elever, särskilt stöd och åtgärdsprogram samt disciplinära åtgärder, även en hel del beslut som får överklagas av elev/vårdnadshavare.

Men som vi ovan också har nämnt är rättsliga grunden allmänt intresse oftast också tillämplig eftersom de olika uppgifterna också ingår i uppgiften att anordna utbildning.

Intresseavvägning (Art 6.1 f)

I vissa fall får den personuppgiftsansvarige behandla personuppgifter utan samtycke om den personuppgiftsansvariges intressen väger tyngre än den registrerades och om behandlingen är nödvändig för det aktuella ändamålet för att fullgöra sina uppgifter. Denna grund kan inte myndigheter/kommunala skolor tillämpa, däremot friskolor. Men

man behöver göra en noggrann bedömning eftersom uppgifter om barn anses vara särskilt skyddsvärda. I de allra flesta fall kommer andra rättsliga grunder att vara tillämpliga, intresseavvägning blir sannolikt därför sällan aktuellt.

Samtycke (Art 6.1 a)

GDPR ställer särskilda krav på utformningen samtycket. Samtycke ska inhämtas för varje särskilt syfte, vara klart och tydligt samt ges efter att den registrerade har fått information om personuppgiftsbehandlingen. Ett samtycke får alltså inte vara för omfattande. Dessutom ska det vara frivilligt och samtycket kan alltid återkallas, vilket man också behöver informera om. Som personuppgiftsansvarig måste man kunna bevisa att samtycke har inhämtats, se till att det finns rutiner för att dokumentera och bevara dessa. För barn och elevers räkning behöver båda vårdnadshavarnas samtycke inhämtas. Om samtycket återkallas, innebär det inte att tidigare hantering blir olaglig, däremot får förskolan/skolan inte fortsätta hantera personuppgifterna.

Möjligheten att använda samtycke är begränsad och ska därför bara användas i undantagsfall. Man måste därför alltid först överväga om personuppgiftsbehandlingen har stöd i någon av de andra rättsliga grunderna. IMY anger följande på sin webb:

Samtycke kan vanligtvis inte användas som rättslig grund för behandling av personuppgifter i skolan. Samtycke kan inte utgöra giltig rättslig grund när det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvariga och det därför inte är sannolikt att samtycket har lämnats frivilligt. Ett sådant ojämlikt förhållande är det oftast mellan en elev och skolan. Samtycke kan därför användas endast vid behandling av personuppgifter som sker utanför skolans ordinarie verksamhet, exempelvis vid skolfotografering.

De vanligaste situationerna när samtycke således kan vara en lämplig grund är inför fotografering eller att i övrigt lägga ut uppgifter på hemsidan, t.ex. resultat i idrottstävlingar eller liknande, eller för att dokumentera verksamheten i förskola och skola genom film och fotografier. Det sistnämnda framgår av lagstiftningens förarbeten. Ändamålet för behandlingen behöver vara precist uttryckt och man behöver tänka till kring giltigheten av samtycket, dvs. hur länge det ska gälla. Ett inhämtande t ex läsårsvis kan vara en lösning.

Känsliga personuppgifter – viktigt att veta!

Enligt GDPR gäller ett förbud mot att behandla känsliga personuppgifter. Dessa får bara behandlas under vissa omständigheter; det måste finnas både en rättslig grund och ett absolut nödvändigt syfte.

För alla förskolor och skolor finns det förstås behov av nödvändig behandling av känsliga personuppgifter. Det handlar bland annat om olika utredningar inför mottagande i särskolan, att kunna ta emot elever i särskolan eller förskolor och skolor som bara tar

emot elever i behov av särskilt stöd. Det gäller även t.ex. uppgifter i utredningar inom elevhälsan, i arbetet med särskilt stöd och mot kränkande behandling, vid disciplinära åtgärder, erbjudande av modersmålsundervisning och specialkost pga. allergier eller religiös övertygelse samt vid ansökan om tilläggsbelopp med mera. Se ovan om begreppet *känsliga personuppgifter.*

För kommunala skolor gäller den svenska dataskyddslagen med bestämmelser för myndigheter att vara tillämplig för behandling av känsliga personuppgifter. För fristående förskolor och skolor, som inte är myndigheter, finns i stället kompletterande regler i 26 a kap. skollagen som innebär att känsliga personuppgifter får behandlas om behandlingen är nödvändig i verksamheten och inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Det gäller i frågor som i stycket ovan anges men även i t.ex. kommunikation om barnets hälsa mellan förskola/skola och föräldrar samt inom elevhälsans psykosociala- och specialpedagogiska verksamhet. Dessutom kan det finnas behov av att behandla personuppgifter som rör lagöverträdelser vid disciplinära åtgärder, t ex. vid avstängning av en narkotikapåverkad elev då man behöver anteckna uppgifter om narkotikabrott samt i andra nödvändiga behandlingar i ärenden, dvs. i löpande text inom elevhälsan och i skriftlig dokumentation som krävs vid disciplinära åtgärder.

Lite mer om några av de grundläggande principerna

Krav på öppenhet - informationskrav
GDPR innehåller krav på att personuppgiftsansvarig ska informera berörda personer om den behandling som sker. Det ska vara klart och tydligt vilka personuppgifter som samlas in och varför. Den rättsliga grunden för behandlingen och ändamålet ska framgå. Man ska även göra informationen lättillgänglig och formulerad med ett klart och tydligt språk.

Ett tips är att göra detta årligen inför höstterminsstart. Föräldrar kan informeras på föräldramöten och/eller i informationsbrev. Information om vilka personuppgifter som behandlas bör alltid ligga på hemsidan.

Komplettera också med kontaktuppgifter till den som är ansvarig om någon har synpunkter, vill rätta uppgifter eller har klagomål. IMY har mer information om vad man behöver tänka på.

Radering av uppgifter

En viktig regel i dataskyddsförordningen är att man inte får spara personuppgifter för länge. När uppgifterna inte längre behövs för det ändamål som de en gång samlades in för, så ska de tas bort. Även med tidigare PUL har rensning varit viktigt att tänka på, men med GDPR infördes utökade möjligheter för privatpersoner att begära radering av uppgifter enligt art. 17, dvs. en rätt att bli bortglömd. Det ska ske utan onödigt dröjsmål. Det finns undantag från rätten till radering om behandlingen är nödvändig för att tillgodose andra viktiga rättigheter som t. ex. för att uppfylla en rättslig förpliktelse,

utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Det innebär att en vårdnadshavare med barn i förskolan och skolan inte kommer att kunna hävda denna rätt så länge barnet/eleven finns kvar i verksamheten. Det kan också finnas skäl för att spara uppgifter pga. av annan lagstiftning eller för att kunna möta andra krav, t.ex. Skolinspektionens krav på att ta del av dokumentation i vissa anmälningsärenden även efter att barnet slutat i verksamheten (gäller framför allt kränkande behandling där utredning kan göras även två år efter det att barnet/eleven slutat). I vår PM om dokumenthantering redogör vi för de olika krav på bevarande av dokumentation som gäller för fristående förskolor och skolor. Ta även gärna hjälp av motsvarande kommunala nämnds dokumenthanteringsplan, där det anges hur länge olika dokument ska sparas och när de får gallras (slängas). Observera dock att olika regler kan gälla för en myndighet och ni som fristående verksamhet, det är viktigt att för sin egen verksamhet tydligt kunna motivera varför uppgifter behöver sparas och ha rutiner för gallring.

Krav på registerförteckning över behandling

Ett första och viktigt steg i att uppfylla kraven i dataskyddsförordningen är att ha kontroll över vilka personuppgifter som hanteras i organisationen. Alla personuppgiftsansvariga är skyldiga att föra en förteckning som anger och beskriver de olika sätt som man hanterar personuppgifter på tillsammans med den lagliga grunden och ändamålet med behandlingen. Förteckningen ska vara tillgänglig i elektroniskt format, t.ex. i ett Excel-kalkylark. Den behöver ses över och uppdateras om man använder personuppgifter för nya ändamål.

Förteckningen ska innehålla följande:

- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.
- Namn och kontaktuppgifter för den personuppgiftsansvarige, den personuppgiftsansvariges företrädare (styrelsen) samt dataskyddsombudet om man har utsett sådan.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.

Säkerhetsaspekter

Man behöver fundera över hur personuppgifterna som hanteras skyddas så att obehöriga personer inte kan komma åt dem. Skyddet kan bestå av tekniska åtgärder som antivirusprogram, brandvägg, trådlöst nätverk med kryptering och datorer med uppdaterade program. Det är också viktigt med organisatoriska åtgärder som exempelvis begränsar vilka anställda som får ta del av olika typer av personuppgifter. Läs mer om säkerhetsfrågorna på IMYs hemsida.

Incidentrapportering

Personuppgiftsincidenter ska anmälas till IMY utan onödigt dröjsmål, inte senare än 72 timmar från kännedom, om incidenten är allvarlig. Även berörda personer måste i vissa fall informeras, om det är stor risk att deras rättigheter och friheter kan påverkas, t.ex. om det finns risk för id-stöld eller bedrägeri. Det här ställer därför krav på att den personuppgiftsansvarige har rutiner för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter. På IMYs hemsida finns mer information om vad som gäller. En personuppgiftsincident kan t.ex. utgöras av att någon i personalen tappar bort ett USB med lagrade personuppgifter, förlorar sin telefon om den använts i arbetet eller om datorer som används i skolan stjäls.

Särskilt om kommunikation via e-post

GDPR innehåller inte några förbud mot kommunicering per mejl. Kommunikation via mejl är naturligt som en del i verksamhetens arbete. Men även här behöver man tänka på att man har en rättslig grund och ett ändamål med behandlingen, som vid vilken annan behandling som helst. Bestäm också hur länge man behöver spara e-post och radera mejlen efter den tiden. Spara aldrig mejl med personuppgifter för att det kan vara bra att ha, för över personuppgifter till andra system och radera mejlet.

När det gäller *känsliga personuppgifter* via e-post måste man vara extra försiktig. Undvik det i möjligaste mån! Om man tänker skicka känsliga personuppgifter, t.ex. en ansökan om tilläggsbelopp till kommunen måste man vara klar över två saker:

1. Har vi tillräckligt hög säkerhet – krypterad e-post rekommenderas!
2. Kan vi säkerställa att mejlet kommer till rätt person? – E-legitimation rekommenderas!
3. Går detta inte att säkerställa – skicka i stället med ordinarie postgång.

Vi länkar nedan till mer information på IMYs webb.

Vad man behöver tänka på och göra!

Hur krångligt är det med GDPR? Mycket av det som regleras i förordningen gällde redan tidigare enligt PUL. Som förskola och skola finns också ofta en vana att ha rutiner för

hantering av personuppgifter, även känsliga sådana. Men med de skarpare kraven och inte minst de nya sanktionsreglerna är det viktigt att sätta sig in i regleringen samt gå igenom och se över rutiner och system.

Några frågor man behöver ställa sig så fort det gäller hantering av uppgifter om personer:

- Är det personuppgifter?
- Är det behandling? Uppfyller behandlingen ett nödvändigt syfte?
- Vad har vi för rättsligt stöd för behandlingen?
- Är behandlingen tillräckligt säker?
- Måste allt verkligen sparas, hur länge behöver vi spara uppgifterna och när ska vi radera?

Checklista

- Inventera vilka personuppgifter som finns i era olika system.
- Inventera vilka känsliga personuppgifter som finns.
- Vilket rättsligt stöd finns för behandlingen? Är ändamålet tydligt och klart?
- Tänk på att även bilder och alla andra uppgifter som kan knytas till en person är personuppgifter på webb och i andra sammanhang.
- Bestäm hur länge de olika personuppgifterna ska sparas. Observera att det kan finnas annan lagstiftning som ställer krav på viss tid (se bl a vår PM om dokumenthantering)
- Se till att ha rutiner för rensning.
- Upprätta en registerförteckning av vilka typer av uppgifter det handlar om samt hur de används, t.ex. i ett Excel-kalkylark.
- Se över nuvarande samtyckesblanketter så att de överensstämmer med de nya kraven samt er information om samtycke. Det gäller t.ex. för känsliga personuppgifter som erbjudande av specialkost, för fotografering och dokumentation av den pedagogiska verksamheten.
- Besluta om behov av dataskyddsombud.
- Ta fram tydlig information till alla berörda om när och hur personuppgifter samlas in och behandlas samt information om hur man begär rättning och radering. Ange kontaktuppgifter till vem man kan vända sig, dataskyddsombudet eller annan person.
- Säkerställ att uppgifter skyddas på ett bra sätt; genomgång med systemleverantörer för att kunna vidta lämpliga tekniska och organisatoriska

säkerhetsåtgärder för att skydda personuppgifterna, t.ex. brandväggar, krypteringsfunktioner och anti-virus m.m.

- Gå igenom leverantörsavtal för att se om dessa behöver kompletteras med Personuppgiftsbiträdesavtal eller om de behöver förhandlas om pga att det tekniska skyddet i dessa behöver förbättras.
- Ta fram rutiner för agerande vid dataintrång eller annan förlorad kontroll över uppgifter.
- Kan vara bra att också ta fram interna policys och riktlinjer med anledning av ovan.
- Sist men inte minst - Gör all personal medveten om den lagstiftningen och rutinerna!

Några bra länkar med fördjupad information, råd och vägledning

IMY har mycket information på sin hemsida och det är klokt att lite löpande hålla sig informerad. Det finns också annan bra information som vi nedan samlar.

IMY
Tillsynsmyndigheten med informationsansvar https://www.imy.se/
Några exempel från myndigheten:

- Om dataskydd och vad som gäller i olika frågor

https://www.imy.se/verksamhet/dataskydd/
https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/

- Om dataskydd inom *skola och förskola*

https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/skola-och-forskola/

- Informationsguider, bl a om personuppgifter i e-post

https://www.imy.se/verksamhet/dataskydd/vi-guidar-dig/

- Om samtycke som rättslig grund

https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/rattslig-grund/samtycke/

Regeringens prop. 2017/18:218 Behandling av personuppgifter på utbildningsområdet
http://www.regeringen.se/rattsdokument/proposition/2018/04/prop.-201718218/

Sveriges Kommuner och Regioner samlade information till kommunerna
https://skr.se/skr/ekonomijuridik/juridik/offentlighetsekretessarkivdataskyddsforordningengdpr/dataskyddsforordningengdpr.13023.html

Svenskt Näringslivs information om dataskyddsförordningen för företag
https://www.svensktnaringsliv.se/fragor/digitalisering/foretagen-och-dataskyddsforordningen-nya-regler-for-hantering-av_670508.html

Guide med generell information för företagare framtagen av **Verksamt och IMY**
https://www.verksamt.se/driva/gdpr-dataskyddsregler/gdpr-guiden

På https://www.dinsakerhet.se/ har **Myndigheten för samhällsskydd och beredskap** samlat fakta om informationssäkerhet och hur du som privatperson kan skydda din integritet.

På **Surfa lugnt** https://surfalugnt.se/ finns råd och tips om hur man kan stötta barn och ungdomar till att använda internet på ett säkert och tryggt sätt.

AcadeMedia har också mycket information om GDPR på sitt öppna intranät, bland annat information till elever och vårdnadshavare samt policys, riktlinjer och rutiner för sin verksamhet. https://trygg.academedia.se/

På **vår egen webb** finns också en särskild pm om **PUB-avtal** som innehåller en genomgång av vilka faktorer som påverkar om en organisation är att anse som personuppgiftsansvarig – ensam eller tillsammans med någon annan – eller som ett biträde. Även några exempel som rör just förskola och skola.
https://www.friskola.se/2018/12/18/personuppgiftsansvar-personuppgiftsbitradesavtal-eller-gemensamt-ansvar-inom-skolvasendet/

Svenskt Näringsliv har också information om personuppgiftsbiträdesavtal
https://www.svensktnaringsliv.se/sakomraden/digital-policy/rapport-om-rollfordelning-for-korrekt-personuppgiftsansvar_1004461.html

Förbundsjuristerna/MD
Uppdaterad
2022-09-27