GDPR – policy

1. Syftet med policyn

Denna policy är framtagen av Läromedelsföretagen i anledning av särskilda frågor som uppkommer i sådana företags verksamhet, och i synnerhet om överföring av personuppgifter till tredje land. Policyn är inte en generell redogörelse av innehållet i Dataskyddsförordningen. För sådana hänvisas i första hand samt till Integritetsskyddsmyndighetens (IMY, tidigare Datainspektionen) hemsida samt till direktivet som sådant.

2. Allmänt om GDPR

Dataskyddsförordningen (GDPR) är ett EU – direktiv som är till för att skydda enskildas personuppgifter. Den har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter. Lagen ställer en rad krav på den part som hanterar personuppgifter.

Personuppgifter är all slags information som kan knytas till en levande person. Namn, adress och personnummer är uppenbart personuppgifter. Även foton på personer och klassas som personuppgifter och ljudinspelningar kan vara det. Resultat på prover och tester, uppgifter om frånvaro eller uppgifter om genomgångna kurser är personuppgifter om de kan knytas till en enskild person. Om man genom att kombinera ett antal olika uppgifter kan sluta sig till vem en icke namngiven person är så rör det sig också om personuppgifter.

Anonymiserade uppgifter och aggregerad statistik som inte kan härledes till en person är i regel inte personuppgifter.

Vid behandling av personuppgifter gäller enligt GDPR att behandlingen ska vara laglig, korrekt och öppen i förhållande till dem vars personuppgifter behandlas. Uppgifterna får bara behandlas för de ändamål som angivits av den personuppgiftsansvarige. De uppgifter som behandlas får inte vara alltför omfattande i förhållande till ändamålet (uppgiftsminimering). Uppgifterna får inte sparas längre än nödvändigt och de ska skyddas mot otillåten eller obehörig åtkomst eller behandling.

I Sverige kompletteras Dataskyddsförordningen av Dataskyddslagen (Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning).

2.1 Undantag för tryck- och yttrandefrihet

Tryckfrihetsförordningen och Yttrandefrihetsgrundlagen utgör svensk grundlag. I Dataskyddslagen tydliggörs det att Dataskyddsförordningen inte ska tillämpas i den utsträckning det skulle strida mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Vidare anges att ett antal centrala bestämmelser i GDPR inte ska tillämpas vid behandling av personuppgifter som sker för journalistiska ändamål eller för akademiskt, konstnärligt eller litterärt skapande.

Ett läromedels innehåll kan därför inte angripas med stöd av Dataskyddsförordningen. Även förberedande material såsom manus och minnesanteckningar omfattas av detta skydd.

2.2 Personuppgiftsansvarig och Personuppgiftsbiträde

Den som behandlar personuppgifter är antingen Personuppgiftsansvarig eller Personuppgiftsbiträde. Med Personuppgiftsansvarig menas den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Med Personuppgiftsbiträde menas den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Såväl personuppgiftsansvariga som personuppgiftsbiträden är verksamheter, i regel företag eller myndigheter. Privatpersoner, redaktörer, lärare eller skolledare är i regel inte ansvariga eller biträden i Dataskyddsförordningens mening.

Medlemsföretagen uppträder ofta såväl i rollen som ansvarig som i rollen som biträde, och det är också vanligt att ett biträde i sin tur anlitar ett underbiträde. Det är viktigt att tänka igenom i vilken roll man uppträder i respektive sammanhang.

3 Särskilt om personuppgiftsbiträden i förhållande till skolans verksamhet

Skolan behandlar personuppgifter om sina elever för att tillhandahålla, anordna och bedriva undervisning. Detta är personuppgiftsbehandlingar som är nödvändiga för att utföra en uppgift av allmänt intresse. När skolan använder digitala lärresurser och läromedel så är skolan ansvarig för den personuppgiftsbehandling som följer. De som tillhandahåller sådana lärresurser och läromedel är att se som biträden.

En vanlig situation är att en skola köper in ett visst läromedel, digitalt eller med digitala inslag. För åtkomst krävs det i regel att läraren, ibland eleverna själva, registrerar ett konto med login och lösenord. Vilka ytterligare uppgifter som krävs och i vilken utsträckning de ska vara tvingande är en fråga för varje enskilt förlag i dialog med sina kunder. Observera dock principen om uppgiftsminimering; Personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet. Man bör således avstå från att samla in mer uppgifter än vad som behövs. Personuppgifter om barn är särskilt skyddsvärda eftersom barn kan ha svårare att förutse riskerna med att lämna ifrån sig uppgifter och förstå vilken rätt de har till skydd för sina uppgifter. Förlagen bör därför vara särskilt försiktiga med sådant insamlande och visa en lyhördhet till synpunkter kring detta.

I syfte att begränsa administrationen för såväl skolor som för förlagen rekommenderar vi att man strävar efter att sluta avtal med så övergripande enheter som möjligt, exempelvis kommunens utbildningsförvaltning snarare än med enskilda skolor. Organisation och namn på sådana enheter skiljer sig mellan kommuner.

Övervägandena blir i princip desamma för det fall det handlar om en friskola.

3.1 Sveriges kommuners och regioners mall

I syfte att underlätta kommunernas arbete med Personuppgiftsbiträdesavtal har SKR tagit fram en mall, vilken förbättrats i ett par omgångar. Nu aktuell version benämns 1.2.1.

Till avtalet hör en instruktion från den ansvarige till biträdet, vilken dock i praktiken ofta fylls i av biträdet. Individuella anpassningar och avsteg från avtalets bestämmelser görs också i regel i bilagan. Man bör exempelvis mot bakgrund av punkt 10.2 överväga att i avtalet ange att löpande uppgraderingar och felsökningar görs rutinmässigt utan att det meddelas ansvarig.

För ett väl fungerande integritetsskydd är det viktigt att båda parter inte bara ser Personuppgiftsbiträdesavtalet som en formalitet, utan att man i samband med avtalets ingående gemensamt analyserar vilka dataflöden som finns, vilka uppgifter som behandlas för vilka ändamål och på vilka grunder, huruvida några av dessa är känsliga samt vilka underbiträden som förekommer i flödet. Kommunernas kompetens på området varierar, och här har vi möjlighet att utgöra ett stöd i deras verksamhet.

4. Överföring av uppgifter till tredje land

Genom dataskyddsförordningen har alla EU:s medlemsstater och EES-länderna ett likvärdigt skydd för personuppgifter. Därför kan personuppgifter föras över fritt inom detta område.

För överföringar utanför EU/EES, exempelvis USA, saknas det däremot generella regler som ger motsvarande garantier. För överföringar till sådana länder finns det istället ett antal mekanismer. Tänk på att en överföring inte bara behöver innebära ett aktivt skickande av uppgifter till exempelvis en server i USA. Support eller underhåll som vidtas därifrån kan innebära att uppgifter överförs.

4.1 Adekvat skyddsnivå

EU-kommissionen kan bedöma att ett visst land utanför EU/EES säkerställer så kallad adekvat skyddsnivå. Israel och Japan är två exempel. En uttömmande lista finns på IMY:s webbplats.

En personuppgiftsansvarig eller ett biträde kan däremot inte göra den bedömningen på egen hand.

USA, som är centralt när det handlar om IT-tjänster, anses inte hålla en adekvat skyddsnivå. Tidigare fanns det ett arrangemang för överföring av personuppgifter mellan USA och EU (Privacy shield). Detta underkändes dock i juli 2020 i en dom kallad Schrems II. Skälet till underkännandet var att den amerikanska lagstiftningen bland annat möjliggör övervakning på ett sätt som inte ansågs förenligt med GDPR.

4.2 Bindande företagsbestämmelser

Bindande företagsbestämmelser (Binding Corporate Rules, BCR) är regler som framför allt multinationella koncerner kan ta fram för att reglera sin behandling av personuppgifter och säkerställa lämpliga skyddsåtgärder vid överföring av personuppgifter till företag inom den egna koncernen i länder utanför EU/EES. Bindande företagsbestämmelser måste godkännas av ansvarig europeisk dataskyddsmyndighet, exempelvis Integritetsskyddsmyndigheten.

4.3 Standardavtalsklausuler

EU-kommissionen har utfärdat standardavtalsklausuler som man kan använda i förhållandet mellan den som överför uppgifter från EU/EES till en mottagare utanför EU/EES. Klausulerna, som är omfattande, kan antingen arbetas in i parternas ordinarie avtal eller användas som en separat bilaga. Klausulerna kan i enskilda fall behöva kompletteras med ytterligare skyddsåtgärder av mer teknisk

natur. Vissa av de stora amerikanska it-bolagen har arbetat in ellerär är i färd med att arbeta in sådana klausuler i sina avtal.

4.4 Storbritannien

För Storbritannien gäller en tillfällig lösning som innebär att personuppgifter fortfarande kan överföras fritt från medlemsstater i EU till Storbritannien fram till den 30 juni 2021.

4.5 Rekommendation

Läromedelsförlagen rekommenderar i detta sammanhang sina medlemmar att:

- Skaffa sig en bild av om och hur personuppgifter som förlaget behandlar förs ut utanför EU/EES

Att i så fall i möjligaste mån undvika sådana överföringar genom att antingen istället anlita aktörer inom EU/EES eller använda sig av de regionala lösningar som erbjuds i kombination med avtalsklausuler som förbjuder överföring utanför regionen. För det fall man istället önskar överföra personuppgifter utanför EU/EES har Europeiska dataskyddsmyndigheten tagit fram riktlinjerna: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

5. Insamling av personuppgifter för marknadsföringsändamål

Behandling av personuppgifter för marknadsföringsändamål kan normalt ske på tre grunder: fullgörande av avtal, berättigat intresse eller samtycke. För känsliga personuppgifter gäller ett krav på samtycke för behandling som huvudregel.

5.1 Fullgörande av avtal

Vid exempelvis köp av en bok måste säljaren behandla adressuppgift för att kunna fullgöra sin del av avtalet, och har således rätt att göra det. Däremot kan man inte sedan fortsätta skicka reklam eller annan marknadsinformation på denna grund.

5.2 Samtycke

För att det ska föreligga ett giltigt samtycke krävs att det är en frivillig, specifik, informerad och otvetydig viljeyttring från individen. Kraven på information är:

• Förlagets identitet,

• ändamålet med behandlingen,

• mottagare eller kategorier av mottagare,

• vilka slags data förlaget kommer att behandla,

• rätten att återkalla samtycket,

• huruvida personuppgifterna kommer att föras utanför EU.

Det ska vara lika lätt att återkalla samtycket som det var att lämna det. Undvik förkryssade samtyckesrutor o.d.

5.3 Berättigat intresse

Berättigat intresse innebär att förlagets intresse att behandla uppgifterna väger tyngre än den berördes intresse av att inte få sina personuppgifter behandlade. Exempelvis så vägs förlagets intresse av att kunna marknadsföra sin utgivning och andra tjänster mot den enskildes integritet. I bedömningen ingår såväl den positiva som negativa effekten av behandlingen för den enskilde, om det finns andra skyddsåtgärder (minimering, avidentifiering, möjligheten att tacka nej till e-post, tekniska och organisatoriska åtgärder för att skydda dem). På denna grund är det möjligt att exempelvis samla in och spara e-postadresser till lärare eller kursföreståndare i utvalda ämnen och sända dem relevant information om kommande utgivning e.d. Anger någon som behandlas enbart på denna grund att denne inte önskar förekomma i ert register ska uppgiften omgående strykas.

Policy fastställd 210507