FRISKOLAN MOSAIK

GDPR-policy
Friskolan Mosaik

180522

Innehåll

1. REGISTRERA PERSONUPPGIFTSBEHANDLINGAR

Personuppgiftsansvarig ansvarar för alla personuppgiftsbehandlingar på Friskolan Mosaik. Alla behandlingar ska finnas i ett register och personuppgiftsansvarig är ansvarig för att registret både är kvalitetssäkrat och uppdaterat.

Registret hjälper oss ha kontroll över vilka personuppgiftsbehandlingar vi utför på Friskolan Mosaik. Det hjälper oss också att, på ett systematiskt sätt, kontrollera att vi till exempel har en rättslig grund att behandla uppgifterna.

Registret är en total kartläggning av alla behandlingar av personuppgifter som utförs på skolan. Det ger en översikt över alla register, system och dokument där personuppgifter förekommer.

Friskolan Mosaiks register finns i digitalt i en mapp där endast ledningspersoner har åtkomst. Här registrerar vi all behandling av personuppgifter, både det som sker i system och manuellt.

2. RAPPORTERA PERSONUPPGIFTSINCIDENTER

Definition

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks.

Exempel:

- diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning
- finansiell förlust
- brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har

- blivit förstörda
- gått förlorade på annat sätt
- kommit i orätta händer.

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter. (Källa: Datainspektionen)

Exempel på incidenter:

- Någon har kommit över ett lösenord som gör att den skulle kunna logga in i system som behandlar personuppgifter.
- Ett mail med känsligt eller extra skyddsvärda personuppgifter skickas till fel mottagare.
- Ett glömt papper i skrivare som innehåller uppgifter om namn och sjukdomstillstånd.
- En dator har fått skadlig kod som gör att obehörig skulle kunna komma åt personuppgifter.

Så här rapporterar du en incident:

En personuppgiftincident ska anmälas till Datanspektionen inom 72 timmar efter att den har upptäckts. Detta gäller även om incidenten inträffat hos ett av våra biträden, det vill säga någon av våra leverantörer. Därför är det viktigt att varje medarbetare rapporterar inträffad personuppgiftsincident.

Alla personuppgiftsincidenter ska rapporteras. Det är viktigt för att vi ska kunna agera vid både allvarliga och mindre allvarliga brister. Varje medarbetare ansvarar för att rapportera risk för, misstanke om eller inträffande av en personuppgiftsincident.

Du rapporterar incidenter på blanketten ”Personuppgiftsincident” och lämnar den till personuppgiftsansvarig.

3. KONSEKVENSBEDÖMNING (DPIA)

Vid personuppgiftsbehandlingar som sannolikt medför en hög risk för den registrerades integritet måste en konsekvensbedömning genomföras.

Den engelska förkortningen som ofta förekommer är DPIA = Data Protection Impact Assessment.

Syfte med bedömningen är att

- förebygga risker innan de uppkommer
- bedöma om personuppgifterna som samlas in är nödvändiga för ändamålet

- bedöma om den personuppgiftsansvarige har vidtagit tillräckliga åtgärder för att skydda den registrerades integritet och rättigheter.

En konsekvensbedömning beskriver syftet med personuppgiftsbehandlingen samt risker som kan uppstå för den vars personuppgifter behandlas.

Konsekvensbedömningen är ett av sätten för den personuppgiftsansvarige att påvisa sin efterlevnad.

En konsekvensbedömning som medför hög risk för den registrerades integritet ska genomföras

- innan vi påbörjar en ny personuppgiftsbehandling
- vid pågående behandlingar som inte konsekvensbedömts tidigare, eller
- vid pågående behandlingar där risken ändrats (ökat).

Ta fram en dataflödesanalys

I en konsekvensbedömning ingår en dataflödesanalys vilket innebär

- en översikt av den funktionella, logiska designen och fysiska designen
- en lista med information om databaser/tabeller/fritextfält som innehåller personuppgifter
- en beskrivning av hur personuppgifter flödar mellan olika parter.

Ett dataflödesdiagram ska tas fram och ses över för livscykelhanteringen av personuppgifter exempelvis insamling, användning, överföring och utlämning samt arkivering alternativt gallring. I diagrammet beskriver vi när vi bör notifiera och få samtycke från den registrerade för personuppgiftsbehandling.

4. PERSONUPPGIFTSBITRÄDESAVTAL (PUB-AVTAL)

Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Ett PUB-avtal är ett avtal som skrivs mellan personuppgiftsansvarig och våra personuppgiftsbiträden. I avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktionerna och att biträdet måste vidta de säkerhetsåtgärder som den personuppgiftsansvarige ska vidta.

5. LAGRINGSMINIMERING, ARKIVERING OCH GALLRING

En av de grundläggande principerna i dataskyddslagstiftningen är principen om lagringsminimering, det vill säga att samla in så få personuppgifter som möjligt. Du får bara samla in de uppgifter som behövs för att kunna utföra arbetet.

Om informationshanteringsplaner och arkivering alternativt gallring

När verksamhetens grund för behandling upphör ska uppgiften arkiveras alternativt gallras. Detta ska framgå i en informationshanteringsplan som ska hållas uppdaterad. Den talar om hur allmänna handlingar hos verksamheten ska hanteras och förvaras.

Det finns många behov att ta hänsyn till och det är inte alldeles lätt att komma fram till när tidpunkten infaller då behandlingen ska upphöra och uppgifterna ska arkiveras alternativt gallras.

Dataskyddsförordningen och arkivering

Arkivering ska ske på separat plats, det vill säga ej i de system du arbetar i.

Dataskyddsförordningen reglerar behandlingen (inhämtande, hantering och lagring) av personuppgifter i verksamheten. Ett syfte är att säkerställa bättre kontroll och säkerhet kring behandlingen.

Offentlighetsprincipen (med reglerna i tryckfrihetsförordningen, offentlighets- och sekretesslagen samt arkivlagen) syftar till att säkerställa allmänhetens tillgång till allmänna handlingar. Dataskyddsförordningen ställer krav på att personuppgifter ska arkiveras alternativt gallras när verksamhetens syfte/grund för behandlingen upphört. Det är därför viktigt att se över och ha väl övervägda tidsfrister i informationshanteringsplanerna.

6. REGISTERUTDRAG

Varje medborgare har rätt att få veta om myndigheten behandlar dennes personuppgifter. Vi är skyldiga att, vid förfrågan, ge ut dessa uppgifter till medborgaren genom ett så kallat registerutdrag.

Ett registerutdrag inkluderar både strukturerad och ostrukturerad data (Word-filer, Excel-filer, enklare listor etc). Undantag finns: ett registerutdrag omfattar till exempel

inte personuppgifter som finns i löpande text som utgör ett utkast eller en minnesanteckning.

Ett registerutdrag ska innehålla:

- Ändamålen med behandlingen.
- De kategorier av personuppgifter som behandlingen gäller.
- De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut,
- Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
- Rätten att av den personuppgiftsansvarige kan begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling.
- Rätten att inge klagomål till en tillsynsmyndighet.

Ta fram texter som klart och tydligt motiverar för medborgaren vilken grund som finns att behandla just denna uppgift.

7. E-POST

Dataskyddsförordningen styr hur personuppgifter får användas/behandlas i samhället. Förändringen påverkar även vår e-posthantering och kräver ett förändrat arbetssätt och våra rutiner kring hantering av personuppgifter i e-post.

Grundregel: Hantering av personuppgifter ska främst ske i system, inte i e-post. Hantering av personuppgifter i e-post räknas också som behandling av personuppgifter och samma krav gäller som för alla andra behandlingar.

Ett e-postmeddelande med personuppgifter får inte ligga kvar i inkorgen eller i skickat-mappen hur lång tid som helst. När behandlingen av personuppgifter är klar ska informationen antingen flyttas över till lämpligt system eller raderas. Den tid som en personuppgift lagras i e-posten ska begränsas till ett strikt minimum.

I e-posten får inte personuppgifter som är känsliga eller sekretessbelagda behandlas eller sparas. Om känsliga eller sekretessbelagda personuppgifter inkommer kan du

till exempel inte vidarebefordra eller svara på mailet när det innehåller uppgifterna. (Läs mer om känsliga uppgifter i filen ”Känsliga uppgifter”).

Skicka aldrig känsliga eller extra skyddsvärda personuppgifter via e-post, till exempel uppgifter om någons hälsa, religiösa åskådning eller politiska åsikter. Undvik även att skicka andra integritetskänsliga och extra skyddsvärda uppgifter som exempelvis lönebesked, värderingar av en person såsom social förmåga eller provresultat via e-post (Läs mer om Extra skyddsvärda uppgifter i filen ”Känsliga uppgifter”).

För över personuppgifter till andra system och radera mejlet. Om en anställd till exempel mejlar in och sjukanmäler sig: registrera det i lönesystemet och radera mejlet. Använd e-post för att kommunicera, inte lagra. Bestäm hur länge personalen behöver spara e-post, flytta eller radera mejlen efter den tiden. Spara aldrig mejl med personuppgifter i gmail "för att det kan vara bra att ha". Informera alla anställda om ovanstående punkter.
Om du måste använda e-post se över om det går det att avidentifiera uppgifterna.

Samma regler gäller vare sig du skickar e-post internt eller externt.

8. SYSTEMSÄKERHET

Alla anställda, uppdragstagare och utomstående användare ska förstå sitt ansvar. Det ska säkerställas att dessa är lämpliga för de roller de anses ha i syfte att minska risken för stöld, bedrägeri eller missbruk av resurser. Det ska också säkerställas att de är medvetna om hot och problem som rör informationssäkerhet samt är rustade för att följa Friskolan Mosaiks regelverk för informationssäkerhet när de utför sitt normala arbete och för att minska risken för mänskliga fel. När anställda, uppdragstagare och utomstående användare lämnar Friskolan Mosaik eller ändrar anställningsförhållande ska det ske på ett ordnat sätt.

Utrustning ska skyddas mot förlust, skada, stöld eller skadlig påverkan på tillgångar och avbrott i vår verksamhet. En grundläggande utgångspunkt är att utrustning såsom datorer, surfplattor, telefoner och likande är arbetsredskap och att användning av dessa ska vara arbetsrelaterad. Användaren har ett förtroende att efter eget gott omdöme använda sig av utrustningen på ett ändamålsenligt sätt. Användaren ansvarar också för att skydda utrustningen mot stöld.

9. BEHÖRIGHET

Princip: Bara den som har rätt att behandla personuppgifter ska kunna utföra denna behandling. Ett grundkrav på system som innehåller personuppgifter är att de går att behörighetsstyra.

Säkerheten kring behörigheter beror mycket på tilldelning och avslutande av behörigheter. Om det dessutom gäller tillgång till känsliga personuppgifter är kraven ännu högre på fungerande rutiner för behörighetshantering och även loggningsfunktioner i systemen, exempel vem som gjorde var och när.

Skapa arbetsrutiner för behörigheter:

- Säkerställ att Friskolan Mosaik har fungerande rutiner även när en medarbetare byter tjänst internt.
- Ha rutiner för att minst årligen kontrollera att behörigheterna är korrekta.
- Kraven på behörigheter gäller även våra leverantörer. Se regelbundet över vilka behörigheten som finns hos våra leverantörer.

10. SAMTYCKE

Samtycke kan bara användas när det verkligen föreligger ett fritt val för den registrerade. Myndighetens ansvar är att visa att den registrerade har fått tydlig information och gjort ett fritt och aktivt val att samtycka.
Samtycke till behandling av extra känsliga personuppgifter kräver ett extra tydligt samtycke.

- Se över rutiner där samtycke måste ges. Bygg upp rutiner för att en medborgare ska kunna ta tillbaka ett samtycke.
- Se över de blanketter och de sätt som samtycke ges på idag. Justera våra samtycken så de följer dataskyddsförordningen. De samtycken som tillkommit innan den 25 maj 2018 är endast giltiga om de följer kraven i dataskyddsförordningen.
- Se över om det finns några samtycken, både blanketter och i system, som kan tas bort. Principen är att inte begära in samtycke om man redan har en rättslig grund för behandling.

11. INFORMATIONSPLIKT

Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) hos den personuppgiftsansvarige och det finns risk för till exempel identitetsstöld eller bedrägeri.

Informationen ska tillhandahållas den registrerade kostnadsfritt i en lättillgänglig, skriftlig form (vilket kan vara i elektronisk form) och med ett tydligt och enkelt språk. I dataskyddsförordningen anges utförligt vilken information som ska ges. Bland annat ska information lämnas om kontaktuppgifter till den personuppgiftsansvarige, den rättsliga grunden för behandlingen och ändamålet med behandlingen.

Om personuppgifter som rör en registrerad person samlas in ska följande information lämnas;

- Kontaktuppgifter för den ansvariga verksamheten
- Ändamålen med behandlingen
- Den rättsliga grunden för behandlingen
- Den period personuppgifterna kommer att lagras
- Den registrerades rättigheter såsom rätten att bli bortglömd

12. EFTERLEVNAD

Vi ska kunna visa att vi följer Dataskyddsförordningen. Omvänd bevisbörda tillämpas. Det innebär att Datainspektionen (som är tillsynsmyndighet) inte behöver visa att vi gjort fel, utan vi måste istället visa att vi gjort rätt.

Detta görs bland annat genom att skapa ordning och reda och ha ett strukturerat och medvetet arbetssätt.

Ett effektivt sätt att visa på efterlevnad av lagen är att dokumentera det vi gör, till exempel genom att arbeta utifrån områdena som beskrivits ovan och dokumentera utfallet. Exempel på dokumentation:

- register över personuppgiftsbehandlingar
- dokumenterade konsekvensbedömningar
- informationshanteringsplaner
- säkerhetsskyddsanalyser
- klassningar av system
- beslutsunderlag till varför vi valt att hantera personuppgifter på ett visst sätt
- åtgärdsplaner
- utförda åtgärder vid incidenter
- kravställning på systemleverantörer
- PUB-avtal i enlighet med dataskyddsförordningen.