Checklista inför att den nya Dataskyddsförordningen, GDPR, träder i kraft den 25 maj 2018. Detta är i princip taget från SKLs checklista.

1. **Förbered verksamheten**

- Skolan bör försäkra sig om att beslutsfattare, medarbetare och nyckelpersoner inom skolan är medvetna om att dataskyddsförordningen kommer att ersätta personuppgiftslagen (PUL).
- Skolan bör också undersöka hur er organisation kommer att påverkas av förordningen och identifiera de områden som skolan måste arbeta särskilt med.

2. **Organisera GDPR-arbetet**

Se till att det finns en organisation på plats som kan arbeta med dataskydd.

En nyhet med det nya regelverket är att den personuppgiftsansvariga organisationens ansvar för att driva dataskyddsarbetet tydliggörs. Det finns även flera nya krav på att skolan måste kunna visa upp att man följer regelverket och hur man följer det.

- Se över den interna styrning och riktlinjer för hur personuppgifter hanteras
- Se till att det finns en organisation med utpekat ansvar och roller som inte enbart är en projektorganisation utan ger förutsättningar för att kontinuerligt arbeta med området.

3**. Kartlägg**

Ta reda på vilka personuppgiftsbehandlingar som finns i skolan och upprätta en registerförteckning.

- Inventera och dokumentera vilka personuppgifter skolan hanterar, hur de samlas in och till vem uppgifterna lämnas ut.
- Gör en bred översyn för att ta reda på vilka uppgifter som hanteras inom de olika delarna av skolan.

- Upprätta en registerförteckning över alla personuppgiftsbehandlingar. Om det finns en registerförteckning enligt personuppgiftslagen behöver den kompletteras och uppdateras.
- Se över rutiner och instruktioner så att det inte blir ett engångsarbete utan att registerförteckningen kan hållas kontinuerligt uppdaterad.

För att kunna säkerställa att personuppgifter i skolan hanteras på rätt sätt och kan skyddas, är det grundläggande att ha uppdaterad kunskap om vilka behandlingar som finns och som tillkommer och förändras löpande. Reisterförteckningen ska fungera som ett nav för arbetet med dataskydd.

Dataskyddsförordningen innehåller dessutom flera rättigheter för individer som ska kunna garanteras i ett informationssamhälle. För att säkerställa att de registrerade kan ta tillvara sina rättigheter är det även en förutsättning att kunna hitta uppgifter om enskilda individer för att till exempel genomföra rättelser eller kunna redovisa till vilka andra uppgifter har lämnats ut.

4. **Analysera**

Ta reda på vilka rättsliga grunder ni har för att behandla personuppgifter. Vilka skyddsåtgärder behövs och vilka risker kan finnas?

- Ta reda på vilka rättsliga grunder som tillåter att personuppgifter får behandlas för varje behandling.
- Se till att detta dokumenteras i registerförteckningen.
- Om personuppgifter behandlas med stöd av samtycke, se till att det i efterhand kan visas att ett giltigt samtycke har lämnats.
- Genomför konsekvensanalys för behandlingar med särskilda integritetsrisker.

Konsekvensanalys måste göras vid behandlingar där personuppgifter om hälsa, etniskt ursprung, politisk uppfattning, medlemskap i fackförening eller andra särskilt känsliga kategorier av uppgifter behandlas i stor omfattning.

Det nya regelverket medför flera förändringar och en sådan som kan få stor praktisk påverkan gäller just vilka grunder för behandling som finns. En viktig ändring när det gäller behandling av personuppgifter i löpande text är att ett undantag som fanns i PuL, den så kallade missbruksregeln nu försvinner. Det innebär bland annat att man nu måste dokumentera vilken rättslig grund som ger stöd för att behandla även personuppgifter som finns i löpande text och i annan ostrukturerad form.

5. **Dokumentera**

Samla systematiskt och fortlöpande dokumentation som visar hur skolan följer dataskyddsförordningen, utöver registerförteckningen.

- Besluta en övergripande policy för dataskydd som beskriver mål, styrning, organisation och ansvar för dataskyddsarbetet.
- Se till att dokumentation om dataskydd hålls på ett ordnat och systematiskt sätt och att rutiner finns för att hålla det uppdaterat.
- Samla bevis för hur reglerna följs.

Dataskyddsförordningen ställer krav på att den personuppgiftsansvariga organisationen ska kunna visa att man följer reglerna och även hur man följer reglerna. Detta kräver utöver registerförteckningen och konsekvensanalyser att flera analyser ska dokumenteras, till exempel riskanalyser om säkerhetsåtgärder.

6. **Inför nya rutiner**

Se till att förberedelsearbetet tar sikte på att arbetet med dataskydd ska fungera kontinuerligt i skolan.

- Planera för att skolan ska kunna upprätthålla ett långsiktigt arbete kring dataskydd.
- Se även över befintliga processer och styrdokument för nära liggande processer som t.ex. informationssäkerhet, dokument- och ärendehantering, upphandling, systemförvaltning och IT-drift så att de vid behov kompletteras med dataskyddsåtgärder.
- Påbörja arbetet med inbyggt dataskydd, ”Privacy by Design”, i verksamheten inför upphandlingar av system och tjänster och vid utveckling.

- Förbered rutiner för att kunna upptäcka och anmäla personuppgiftsincidenter.

7. **Leverantörer och avtal**

Se till att avtal med leverantörer och pågående upphandlingar har tillräckliga krav på åtgärder för dataskydd.

- Se över aktuella avtal och säkerställ att de är uppdaterade med personuppgiftsbiträdesavtal och instruktioner som är anpassade till dataskyddsförordningen.
- Kontrollera att pågående upphandlingar tar med aktuella krav och personuppgiftsbiträdesavtal.
- Ta kontakt med leverantörer för att säkerställa att kunskap om det nya regelverket finns och att det finns samstämmighet om roller och ansvarsfördelning.

8. **Säkerställ individens rättigheter**

Se till att det arbete med dataskydd som genomförs i organisationen genomsyras av att de registrerade individernas rättigheter är i fokus.

- Se till att skolan har rutiner på plats för att säkerställa att vi kan uppfylla alla rättigheter som de registrerade har enligt dataskyddsförordningen.
- Se till att det finns information på webbplatsen eller på andra kontaktytor så att individer kan få information om de behandlingar som utförs, om de registrerades rättigheter och hur de kan utöva dem.

De viktigaste rättigheterna för de registrerade är att:

- Vid begäran få tillgång till sina personuppgifter.
- Få felaktiga personuppgifter rättade.
- Kunna få sina personuppgifter raderade (här finns omfattande undantag för myndigheter).
- Ha möjlighet att invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering.