



Så hanterar du information och personuppgifter

Beroende på vilka typer av personuppgifter vi hanterar så finns det olika regler för var vi ska hantera dem, vilket skydd de behöver och vilka som får se uppgifterna. Dataskyddsförordningen (GDPR) ger vägledning för hur detta ska gå till. Ju känsligare uppgifter desto högre krav i lagstiftningen.

I tjänsten har vi rätt att använda de personuppgifter som vi behöver, men det är inte samma sak som rätt att sprida dem till andra! Därför ska vi alltid vara mycket försiktiga i vår hantering av uppgifter och alltid ha full kontroll på vilka som kan se.

Rent praktiskt kan vi dela in personuppgifter i fyra kategorier, där vi tilldelar en färg till varje för en tydligare vägledning:

1. Blå uppgifter – uppgifter som vi vill sprida eller få publik reaktion på genom sociala medier eller webb.

På öppna platser eller tjänster där alla kan se, som sociala medier och webbplatser, ska du publicera så lite personuppgifter som möjligt. Var mycket försiktig då uppgifterna kommer att spridas utanför din kontroll. Sträva efter att det är valbart att medverka i sådan publicering. Håll dig till ett minimum av personuppgifter som namn, ålder, roll, skola/arbetsplats.

Det är tillåtet med identifierbara personer i bild/film när du informerar om verksamheten men tänk på integritet och att barns uppgifter har ett extra högt skyddsvärde. All publicering ska ske av personer som i förväg är utsedda för det.

2. Gröna uppgifter – uppgifter som används för samarbete och information internt, ibland externt.

När du hanterar personuppgifter internt som inte är integritetskänsliga kan du använda tjänster och platser som exempelvis M365 och Google Workspace samt olika läromedels-tjänster. Du får inte hantera alla typer av uppgifter och ska hålla dig till platser där delningen av uppgifter sker på ett genomtänkt och välordnat sätt.

Det finns många tjänster som inte fullt ut följer GDPR och till exempel hanteras utanför EU/EES och då bör du inte hantera personuppgifter alls i de tjänsterna eller apparna. Hör alltid efter med din chef innan du börjar behandla denna typ av uppgifter på ett nytt sätt.

3. Gula uppgifter – verksamhetens viktiga uppgifter som vi ska skydda och använder i dagligt arbete internt.

Om du ska hantera skyddsvärda eller integritetskänsliga uppgifter finns det oftast redan ett uttänkt och avsett system, tjänst eller plats för ändamålet. Det är vanligt att det finns en huvudansvarig utsedd för hanteringen.

Skyddet ska vara starkt och det ska vara full kontroll över vilka som kan se uppgifterna. Om det införs en ny tjänst för denna typen av uppgifter finns det mycket att tänka på för att säkerheten ska vara tillräcklig - kontakta avtalsansvariga eller samordnare för personuppgiftsfrågor på förvaltningen!

4. Röda uppgifter – uppgifter som kan orsaka stor skada om de sprids till oberoende, ska endast hanteras internt.

När du hanterar känsliga personuppgifter, integritetskränkande eller skyddade uppgifter ska det ske på ett redan fastställt sätt och finnas stöd för hanteringen i lag. Vi ska inte påbörja nya sätt att behandla denna typen av uppgifter utan att göra en större konsekvensanalys med jurister och andra sakkunniga.

Om du hamnar mellan två kategorier i ditt tänk, använd riktlinjerna för den striktare kategorin.

Försök inte att komma på genvägar för en mer tillåtande hantering, då det motverkar hela syftet med att skydda uppgifter på ett säkert sätt.

Tabell - Så hanterar du information och personuppgifter

Kategori	Blå uppgifter – uppgifter som vi vill sprida eller få publik reaktion på	Gröna uppgifter – uppgifter som används för samarbete och information internt, ibland externt	Gula uppgifter – verksamhetens viktiga uppgifter som vi ska skydda och använder i dagligt arbete, mest internt	Röda uppgifter – uppgifter som kan orsaka stor skada om de sprids till oberoende och som vi bara ska hantera internt
Syfte	Att informera och inspirera, riktat mot bred allmänhet och målgrupper	Att samarbeta, kommunicera, utbilda, lära sig, ta del av innehåll, som riktas till utvalda målgrupper	Att driva verksamheten, hantera processer och ärenden för de som har dessa arbetsuppgifter	Att hantera uppgifter där det finns höga krav på säkerhet enligt lag
Typ av uppgifter	Publik information, nyheter, event, offentliggjorda uppgifter	Ikke integritetskänsliga uppgifter, arbetsmaterial, administrativa uppgifter, pedagogiskt arbete	Integritetskänsliga, skyddsvärda uppgifter, uppgifter med förväntad svag sekretess	Känsliga personuppgifter, uppgifter med förväntad stark sekretess
Typ av system eller tjänst	Sociala media, webbplatser, pod-tjänster	Samarbetsverktyg, innehållstjänster, läromedel, verktyg och appar, enkla online-tjänster och IT-tillägg	Verksamhetssystem och lagringsplatser på stadens servrar	System för känsliga uppgifter som journaler, elevakter, stödinsatser, medicinskt stöd
Exempel på system eller tjänst	YouTube, Facebook, Instagram och liknande kanaler	Google Workspace for Education, Microsoft Teams (365) och liknande molntjänster, läromedelstjänster	Unikum, Itslearning, Tempus, Skola24, Edlevo, HR-system, lagring på stadens servrar	Prorodata, DF Respons, Unikum stödmodul, lagring på stadens servrar
Exempel på uppgifter som hanteras	• enstaka för- och efternamn • skolenhet, arbetsplats • yrke, roll • ålder • kontaktuppgifter (vuxna) • Identifierbar person i bild/film - alla i syftet informera om den dagliga verksamheten som en del i myndighetens uppdrag	• listor med för- och efternamn • adressuppgifter • födelseår (ÅÅMMDD) • enstaka formative elevbedömningar, ej tillsammans med helt personnummer • enstaka mätuppgifter, ej tillsammans med helt personnummer • publika organisationsuppgifter • mötesinbjudningar • publikt informationsmaterial • politiska beslut och protokoll • avtal utan sekretess • presentationer • arbetsmaterial	• helt personnummer kopplade till andra personuppgifter • lön och uppgifter om anställning • användarnamn • uppgifter om lagöverträdelse • värderande uppgifter, till exempel uppgifter i medarbetarsamtal, resultat från personlighetstester/ profiler • summative elevbedömningar • samlade mätuppgifter • information från någons privata sfär • uppgifter om sociala förhållanden • incidentrapporter • krisledning/risk och sårbarhetsanalyser • systeminformation, teknisk struktur	• uppgifter om enskilda hälsotillstånd, andra personliga förhållanden inom hälso- och sjukvård • skyddade personuppgifter • upphandlingsunderlag • uppgift om enskilda förhållanden inom förskolan • utredningar med känsliga personuppgifter • etniskt ursprung • politiska åsikter • religiös/filosofisk övertygelse • medlemskap i fackförening • sexualliv eller sexuell läggning • biometriska uppgifter som ansikts-igenkänning, DNA och fingeravtryck • information om säkerhetsskydd • information om samhällsviktiga system
Hur du får använda personnummer	Inte alls	Använd födelseår i formen ÅÅMMDD i stället för helt personnummer och endast med administrativa uppgifter som enhet, klass, kurs, övergripande ändamål och annan enstaka uppgift	Personnummer får kopplas till andra personliga och skyddsvärda uppgifter men inte till känsliga personuppgifter	Personnummer får även kopplas till känsliga personuppgifter