2021-03-10 Dnr SBB2021-221

Maria Larsson

Förslag till Personuppgiftsstrategi och Riktlinjer för behandling av personuppgifter

Förslag till beslut

Direktionen beslutar att anta Personuppgiftsstrategi samt Riktlinjer för behandling av personuppgifter för Samhällsbyggnadsförbundet Bergslagen.

Beskrivning av ärendet

Sedan den 25 maj 2018 gäller EU:s dataskyddsförordning. Denna strategi beskriver förbundets hantering av personuppgifterna på övergripande nivå för att säkerställa att kraven i dataskyddsförordningen samt övrig gällande rätt på området följs. Strategin gäller vid all behandling av personuppgifter inom förbundet och kompletterar övriga styrdokument.

Personuppgiftstrategin är ett dokument som redovisar förbundets övergripande mål och inriktning avseende hantering av personuppgifter. Dokumentet ”Riktlinjer för behandling av personuppgifter” konkretiserar personuppgiftsstrategin med mer detaljerad information och regler för hur personuppgifter får hanteras inom förbundet.

Strategin och riktlinjerna gäller för förbundet, direktionen, avdelningar, medarbetare och förtroendevalda politiker. Eftersom alla verksamheter omfattas av strategin och riktlinjerna finns inte utrymme för att besluta om lokala regler som avviker från dessa.

För ärendet aktuella handlingar

Personuppgiftsstrategi för Samhällsbyggnadsförbundet Bergslagen
Riktlinje för behandling av personuppgifter för Samhällsbyggnadsförbundet Bergslagen

Samhällsbyggnadsförbundet Bergslagen

Maria Larsson
Arbetsledare Servicecenter

Riktlinje för behandling av personuppgifter

För Samhällsbyggnadsförbundet Bergslagen

Antagen av direktionen 2021-XX-XX

Innehållsförteckning

1. Inledning

Sedan den 25 maj 2018 gäller EU:s dataskyddsförordning (nedan dataskyddsförordningen). Förordningen innehåller bland annat regler om när personuppgifter får samlas in, hur de får behandlas och hur registrerade ska informeras. Dataskyddsförordningen tillsammans med kompletterande nationella regler, ska tillämpas på all behandling av personuppgifter i förbundet.

Förbundets personuppgiftstrategi är ett dokument som redovisar förbundets övergripande mål och inriktning avseende hantering av personuppgifter. Detta dokument – Riktlinjer för personuppgifter - konkretiserar personuppgiftsstrategin med mer detaljerad information och regler för hur personuppgifter får hanteras inom förbundet.

2. Riktlinjernas omfattning

Denna riktlinje innehåller information och regler gällande hantering av personuppgifter inom förbundet. Riktlinjerna gäller för alla verksamheter i förbundet, vilket medför att det inte finns utrymme att besluta om lokala riktlinjer eller rutiner som avviker från dessa.

3. Undantag och kompletteringar till riktlinjen

Ansökan om undantag från dessa riktlinjer ska ställas till dataskyddsgruppen. Ärenden rörande undantag ska beredas innan de ställs till dataskyddsgruppen för att underlätta beslut. Exempelvis kan en riskanalys ingå i beredningen av ärendet. Undantag från denna riktlinje ska aldrig vara permanenta, utan har en maximal giltighetstid på 2 år. Finns behov om nya undantag ska en ny ansökan lämnas in.

Eftersom ägarkommunerna har många skilda verksamheter kan kompletterande rutiner till riktlinjerna finnas lokalt. Det åvilar respektive verksamhet att ta fram verksamhetsspecifika rutiner och mallar som komplement till de kommunövergripande styrdokumenten. Generella rutiner och mallar kan med fördel tas fram av dataskyddsgruppen. Kompletteringarna får aldrig innebära undantag från riktlinjen om inte ett särskilt tillstånd från dataskyddsgruppen finns. Kontakta ansvarig chef vid osäkerhet om vad som gäller.

4. Viktiga begrepp

Personuppgifter (enligt dataskyddsförordningen) är varje upplysning som avser en identifierad eller identifierbar levande fysisk person (nedan registrerade) såsom exempelvis namn, personnummer och adress. Personuppgifter kan även vara en kombination av uppgifter som tillsammans gör att en person kan bli identifierbar.

Behandling av personuppgifter är ett vidsträckt begrepp och omfattar i princip alla åtgärder som sker i fråga om personuppgifter. Några exempel är insamling, registrering, lagring, läsning och radering.

Personuppgiftsansvarig är den bestämmer ändamålen och medlen med en behandling av personuppgifter, det vill säga varför och hur behandlingen ska gå till. Exempel på personuppgiftsansvariga är styrelser, nämnder, kommunens revisorer och direktionen i ett kommunalförbund.

Personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Biträdet finns alltid utanför den personuppgiftsansvariges organisation, dvs. biträdet är aldrig en anställd hos personuppgiftsansvarig.

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

Registrerade är de fysiska personer vars personuppgifter behandlas.

5. Roller och ansvar

Direktionen

Är ansvarig för framtagande och uppföljning av kommunövergripande styrdokument.

Personuppgiftsansvarig

Personuppgiftsansvarig ansvarar för

- ✓ Att all hantering av personuppgifter som sker i deras verksamhet följer dataskyddsförordningen samt övrig tillämplig gällande rätt.
- ✓ Målen och intentionerna i personuppgiftsstrategin och denna riktlinje efterlevs inom deras verksamhet.
- ✓ Ta fram en handlingsplan för hur de ska arbeta med personuppgifter inom sitt verksamhetsområde.
- ✓ Utse ett eller flera dataskyddsombud samt tillse att kontaktuppgifterna till dataskyddsombuden blir offentliggjorda samt anmäla ett av dataskyddsombudens namn och kontaktuppgifter till tillsynsmyndigheten.
- ✓ Utse flera personuppgiftssamordnare inom förbundet.

Varje personuppgiftsansvarig ansvarar för de straff- och skadeståndsanktioner som kan uppkomma på grund av felaktig behandling av personuppgifter inom deras verksamhetsområde. Om personuppgifter behandlas över gränserna mellan flera personuppgiftsansvarigas verksamheter, ska de personuppgiftsansvariga gemensamt komma överens om hur ansvaret och eventuella sanktionsavgifter ska fördelas. Diarieför överenskommelsen samt dokumentera i GDPR Hero.

Informationssäkerhetssamordnare

Ska leda arbetet med framtagandet av ett inbyggt dataskydd vid behandling av personuppgifter som en del av informationssäkerhetsarbetet.

Objektägare (systemägare)

Objektägare ska finnas för alla system som behandlar personuppgifter. Finns inte någon utpekad objektägare följer ansvaret verksamhetsansvaret. Objektägaren ska tillsammans med förvaltningsledaren skriva en systemförvaltningsplan, där de utifrån det beskrivna ändamålet ska precisera hur de ska uppnå en uppgiftsminimering och lagringsminimering, samt i de fall det görs en konsekvensbedömning (se nedan), vilket dataskydd som krävs.

Förvaltningsledare

Förvaltningsledaren ska förvalta systemet och kontinuerligt informera objektägaren och dataskyddsombudet om händelser och behandlingar som kan påverka den registrerades friheter- och rättigheter på ett negativt sätt. Förvaltningsledaren ska tillsammans med objektägaren skriva en systemförvaltningsplan, där de utifrån det beskrivna ändamålet ska precisera hur de ska uppnå en uppgiftsminimering och lagringsminimering, samt i de fall det görs en konsekvensbedömning (se nedan), vilket dataskydd som krävs.

Dataskyddsombud

Varje personuppgiftsansvarig ska utse ett eller flera dataskyddsombud (varav per personuppgiftsansvarig ska vara anmält till tillsynsmyndigheten). Se även rubriken ” När personuppgiftssamordnare och dataskyddsombud utses ska” under avsnittet ”Personuppgiftssamordnare” nedan.

Dataskyddsombudet/-n ska

- ✓ Alltid sätta dataskydds- och personuppgiftsfrågor främst i förhållande till övriga arbetsuppgifter.
- ✓ Ha mandat att självständigt bedriva sitt arbete utan instruktioner.
- ✓ Ha god kännedom om verksamhetens processer, administrativa rutiner, informationssystem och behov av dataskydd.
- ✓ Informera, utbilda och ge råd till personuppgiftsansvarig och verksamhetens medarbetare i frågor gällande efterlevnad av dataskyddsförordningen och övrig aktuell personuppgiftslagstiftning.
- ✓ På begäran ge råd rörande konsekvensbedömning avseende dataskydd samt övervaka genomförandet av konsekvensbedömningar.
- ✓ Samarbeta samt vara kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling av personuppgifter.
- ✓ Övervaka efterlevnaden av dataskyddsförordningen, annan tillämplig lagstiftning samt interna styrdokument och instruktioner som rör behandling av personuppgifter.
- ✓ Delta som representant i dataskyddsgruppen i egenskap av rådgivare samt för att bidra till nätverkets kompetensutveckling.
- ✓ Rapportera direkt till direktionens ordförande avseende frågor av vikt inom området.
- ✓ Årligen tillsammans med personuppgiftssamordnarna skriftligt (samt muntligt om så önskas) informera direktionens ordförande och personuppgiftsansvariga i förbundet hur arbetet fortlöper och hur dataskyddsförordningen efterlevs.

Personuppgiftssamordnare

Är förbundets huvudsakliga kontaktperson vid frågor rörande personuppgifter och dataskydd och en förmedlande länk till dataskyddsombudet.

Personuppgiftssamordnaren ska:

- ✓ Följa personuppgiftsansvarigs handlingsplan.
- ✓ Registrera pågående behandlingar i registerförteckningen samt löpande följa upp att den verksamhet man representerar har en ifylld och korrekt registerförteckning.
- ✓ Säkerställa att dokumenthanteringsplaner och gallringsrutiner uppdateras när nya personuppgiftsbehandlingar tillkommer och gamla försvinner eller ändras.
- ✓ Samordna den registrerades begäran om registerutdrag utifrån de rutiner som finns inom den egna verksamheten. Rutinerna kan innebära att samordnaren även svarar den registrerade.
- ✓ Utreda och göra förslag till bedömning vid personuppgiftsincidenter. Efter beslut av personuppgiftsansvarig ansvarar samordnaren för att en eventuell anmälan sker till tillsynsmyndigheten via deras e-tjänst.
- ✓ Proaktivt granska verksamhetens personuppgiftsbehandlingar löpande, påpeka eventuella brister och föreslå åtgärder till dataskyddsombud och personuppgiftsansvarig.
- ✓ Ge råd och stöd till verksamhetens ledning och berörda medarbetare i frågor rörande behandling av personuppgifter.
- ✓ Vid behov stödja verksamheten vid upprättande av personuppgiftsbiträdesavtal.
- ✓ Bidra till och ge förslag på gemensamma rutiner inom området.
- ✓ Årligen tillsammans med dataskyddsombudet informera direktionens ordförande och personuppgiftsansvariga i förbundet hur arbetet fortlöper och hur dataskyddsförordningen efterlevs.
- ✓ Vara verksamhetens kontaktperson gentemot dataskyddsombudet.
- ✓ Rådfråga och samråda med dataskyddsombudet.
- ✓ Delta i dataskyddsgruppen.
- ✓ Hålla sig uppdaterad om gällande rätt och andra nyheter inom området personuppgifter och dataskydd.

Uppdraget som personuppgiftssamordnare är primärt inom den egna avdelningen, men arbetsuppgifter kan även förekomma inom andra förvaltningar i kommunen om behov finns p.g.a. frånvaro eller liknande.

<u>När personuppgiftssamordnare och dataskyddsombud utses ska</u>

- ✓ Uppdragen vara fördelade på tillräckligt många personer.
- ✓ De som får uppdragen få tillräckliga resurser i form av exempelvis tid för uppdragen (rimlig arbetssituation) samt tid och ekonomiska resurser för kompetensutveckling inom området.
- ✓ De som får uppdragen ha tillräcklig kompetens inom området personuppgifter och dataskydd eller att det finns en kompetensutvecklingsplan för hur denna kompetens ska uppnås så snart som möjligt.
- ✓ De som får uppdragen ha tillräckliga befogenheter, det vill säga rätt att fatta beslut och vidta åtgärder i enlighet med denna riktlinje samt personuppgiftsstrategin vilket innebär att ändringar i delegationsordningen kan behöva genomföras.

- ✓ Uppdragen vara skriftliga och undertecknas av både den som fördelar och den som tar emot uppgiften.

Dataskyddsgruppen

Är kommunen och förbundets gemensamma nätverk för personuppgifts- och dataskyddsfrågor. Nätverket är till för att stötta verksamheten samt personuppgiftssamordnarna i sitt arbete samt är verksamhetens främsta kontaktyta mellan personuppgiftssamordnare och dataskyddsombud. Sammankallande är kansliets personuppgiftssamordnare.

Deltagarna i dataskyddsgruppen ska vara:

- ✓ Personuppgiftssamordnare i kommunen, förbundet och de kommunala bolagen
- ✓ Informationssäkerhetssamordnaren
- ✓ Dataskyddsombud i kommunen, förbundet och de kommunala bolagen deltar som rådgivare och för att bidra till kompetensutvecklingen, men driver inte arbetet i dataskyddsgruppen.

Utöver ovan nämnda deltagare kan dataskyddsgruppen bjuda in andra deltagare vid behov.

Dataskyddsgruppen ansvarar för att:

- ✓ Ta fram gemensamma riktlinjer, mallar, arbetssätt och rutiner inom området personuppgifter- och dataskydd.
- ✓ Gå igenom personuppgiftsstrategi och riktlinje för behandling av personuppgifter minst en gång per år för att granska om några revideringar behöver ske med anledning av t.ex. ny lagstiftning, ändrad praxis eller nya rutiner inom verksamheten. Vid behov av revidering ska dataskyddsgruppen ta fram en tjänsteskrivelse samt en reviderad utgåva av strategi eller riktlinje och överlämna till kommunstyrelsen? för beslut.
- ✓ Se över om det finns behov av att planera och genomföra gemensamma insatser inom området personuppgifter och dataskydd t.ex. informationskampanjer, utbildningar, frågestunder etc.
- ✓ Besluta om undantag från denna riktlinje efter ansökan från verksamheten.

Upphandlare

Vid upphandling av nya verksamhetssystem ska upphandlaren säkerställa att kraven i dataskyddsförordningen och övrig gällande rätt på området uppfylls under upphandlingens alla faser, dvs. både inför, under och efter upphandlingen.

Inför en upphandling – förstudie

- ✓ Identifiera vilka personuppgifter som kommer behandlas, hur känsliga de är och hur hanteringen kommer att gå till.
- ✓ Kommer känsliga personuppgifter behandlas kan det vara aktuellt med risk- och sårbarhetsanalys och vid en hög risk en konsekvensbedömning.
- ✓ Red ut vilken rollfördelning de olika parterna har, dvs. vem har rollen som personuppgiftsbiträde och vem har rollen som personuppgiftsansvarig. Ofta har leverantören ställning av biträde, men det måste inte vara så varför förhållandet måste vara klarlagt från början.

- ✓ Utred vilka krav som är rimliga att ställa på lämpliga tekniska och organisatoriska skyddsåtgärder i förfrågningsmaterialet.
- ✓ Involvera dataskyddsombudet och informationssäkerhetssamordnaren så tidigt som möjligt.

Upphandlingsdokument
Säkerställ att kommande personuppgiftsbiträden har kompetens, organisation, rutiner och tekniska och organisatoriska möjligheter att skydda personuppgifterna på lämpligt sätt genom att bifoga ett personuppgiftsbiträdes-avtal samt skriva med de krav vi har i upphandlingsdokumentet.

<u>Exempel på saker som ska beaktas i upphandlingsdokumenten</u>
- ✓ Personuppgiftsbiträdesavtal ska finnas med som ett särskilt kontraktsvillkor. Förtydliga att leverantören genom att lämna anbud godtar personuppgiftsbiträdesavtalet.
- ✓ Lämpliga tekniska och organisatoriska säkerhetsåtgärder i förhållande till risken med behandlingen av personuppgifter.
- ✓ Inbyggt dataskydd, dvs. att hänsyn tas till de registrerades integritet i systemet.
- ✓ Dataskydd som standard ska kunna tillgodoses genom att personuppgifter inte ska behandlas i onödan (exempelvis genom att inte mer information än nödvändigt samlas in, delas ut eller visas).
- ✓ Möjlighet att tillgodose de registrerades rättigheter i systemet såsom t.ex. rätt till rättelse, radering, begränsning av behandling, dataportabilitet (i de fall det är aktuellt)
- ✓ Ställ krav på personuppgiftsincidenthanteringen, dvs. hur biträdet ska hantera personuppgiftsincidenter och andra säkerhetsincidenter.
- ✓ Möjlighet att ha en snäv behörighetsstyrning i systemet så att inte behörighet ges i ”klump” till personer som inte behöver uppgifterna för sitt arbete. Kontrollera med de verksamheter som ska använda systemet vilken behörighetsstyrning som behövs.
- ✓ Var personuppgifterna behandlas (t.ex. inom EU/EES eller är även tredje land aktuellt. Om tredje land omfattas krävs specifikationer rörande och i sådant fall krävs adekvat skyddsnivåer för detta.)
- ✓ Om uppförandekoder, certifiering eller standard finns på området så ska en bedömning ske om de ska vara med som krav.

Under upphandlingstiden
Följ upp att avtalet efterlevs utifrån personuppgiftsbiträdets behandling av personuppgifter. Diarieför personuppgiftsbiträdesavtal tillsammans med huvudavtalet.

Medarbetare

Alla medarbetare har ett ansvar för att följa verksamhetens beslutade styrdokument i form av t.ex. strategier och riktlinjer. Varje medarbetare ansvarar även för att följa dokumenthanteringsplaner och gallringsrutiner vilket innebär att bl.a. följa de regler som finns för gallring av e-post, handlingar i pärmar, i personliga och gemensamma lagringsutrymmen på G: eller H: samt vara uppmärksam på brister i hanteringen av

personuppgifter och för att anmäla personuppgiftsincidenter vidare internt. När utbildningsinsatser på området anordnas ska varje medarbetare delta aktivt.

Närmaste chef
Närmaste chef ansvarar för att t.ex. tilldela rätt behörigheter till rätt medarbetare, kontrollera att medarbetarna följer beslutade styrdokument och att de deltar i utbildningsinsatser.

6. Grundläggande principer för behandling av personuppgifter

6.1. Behandlingen ska vara laglig, korrekt och öppen

6.1.1. De lagliga (rättsliga) grunderna i dataskyddsförordningen
Vi får bara behandla personuppgifter om det finns en identifierad och lämplig laglig grund för behandlingen i dataskyddsförordningen (artikel 6). Den lagliga grunden ska vara fastställda innan behandling startar. Vid behandling av känsliga personuppgifter, se även avsnitt 7.1. Utöver att ha en laglig grund så måste övriga principer och bestämmelser i dataskyddsförordningen och annan gällande rätt följas för att behandlingen ska vara laglig.

I dataskyddsförordningen finns 6 lagliga grunder, varav minst en alltid måste vara uppfylld för varje personuppgiftsbehandling. De lagliga grunderna är:

- Samtycke från den registrerade.
- Nödvändig behandling för att fullgöra ett avtal där den registrerade är part eller för att genomföra åtgärder på begäran av den registrerade innan ett avtal ingås.
- Nödvändig behandling för att fullgöra en rättslig förpliktelse
- Nödvändig behandling för att skydda ett grundläggande intresse för den registrerade eller annan fysisk person.
- Nödvändig behandling för att utföra uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- Nödvändig behandling för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre. Denna lagliga grund ska inte användas ska inte gälla för behandling som utförs av offentliga myndigheter när de fullgör sina uppgifter.

Samtycke
Använd bara samtycke som laglig grund om det inte finns någon annan laglig grund. Samtycket måste vara frivilligt och parterna ska vara jämlika för att samtycket ska vara giltigt. Eftersom det ofta finns en maktobalans mellan en myndighet i form av t.ex. en kommun och en medborgare så är det inte en vanligt förekommande laglig grund för de flesta av våra behandlingar.

Ett exempel på när det kan vara aktuellt med samtycke är om vi erbjuder information via e-post om uppdateringar av ett projekt t.ex. vägarbeten, byggande av en park, skola etc. Vi ska då på ett tydligt sätt informera om att det är frivilligt att anmäla sig till e-postutskick och inhämta samtycke för behandlingen av e-postadresserna endast för

detta ändamål. De som inte är intresserade av utskicket kan istället välja att läsa om uppdateringarna på vår webbplats.

Ett samtycke måste inte vara skriftligt, men om det inte är skriftligt så måste det dokumenteras skriftligt eftersom vi måste visa att den registrerade samtyckt till den aktuella personuppgiftsbehandlingen. Vi använder oss därför i första hand av skriftliga samtycken.

Följande information ska finnas dokumenterat vid ett samtycke

- ✓ Hur samtycket inhämtades.
- ✓ När samtycket inhämtades (datum).
- ✓ Vilken information den registrerade fick.

För att det inte ska bli otydligt för den registrerade vad denne ger sitt samtycke till så ska vi undvika att ha med flera andra frågor i samtyckesblanketten. Om fler frågor än själva samtycket finns med så särskilj dessa tydligt.

Använd aldrig förifyllda kryssrutor för ett samtycke, det är den registrerade som själv aktivt ska välja vad denne vill ge samtycke till genom att kryssa i de rutor denne själv väljer.

Den registrerade har alltid rätt att när som helst återkalla sitt samtycke och det ska vara lika lätt att återkalla som att ge sitt samtycke. Säkerställ genom interna rutiner hur den registrerade på ett enkelt sätt ska kunna återkalla sitt samtycke för den aktuella behandlingen. Vid exempelvis e-postutskick kan det finnas med ett stycke i varje utskick om hur man kan återkalla sitt samtycke genom att exempelvis svara på utskicket och berätta att man vill återkalla samtycket.

Precis som vid alla behandlingar av personuppgifter har den registrerade rätt att få information, se avsnitt 8.1. Även om all information ska vara med så var extra tydlig med följande:

- ✓ Vem som begär samtycke, alltså förbundet.
- ✓ Vilken typ av personuppgifter vi tänker behandla, t.ex. e-postadress och namn.
- ✓ I vilket syfte vi vill använda personuppgifterna. Är det fler än ett syfte, beskriv vart och ett.
- ✓ Klargör att det är möjligt att återkalla samtycket samt hur detta kan ske.

Om samtycket riktar sig till ett barn så måste ni kontrollera att informationen är extra tydlig samt att barnet har rättsförmåga att ge sitt samtycke eller om det är vårdnadshavaren som ska lämna sitt samtycke.

6.1.2. Korrekt behandling

All personuppgiftsbehandling ska vara korrekt. Det innebär att den ska vara rättvis, skälig, rimlig och proportionerlig i förhållande till de registrerade.

Personuppgiftsansvarig ska se till att den personuppgiftsbehandling som sker står i rimlig proportion till den nytta som den innebär och hänsyn ska tas till vad den registrerade kan förvänta sig. Personuppgiftsbehandlingen ska vara förståelig och begriplig för de registrerade och inte ske på dolda eller manipulerande sätt.

6.1.3. Behandling på ett öppet sätt

Det ska vara klart och tydligt för de registrerade hur vi behandlar personuppgifter. De registrerade ska få reda på om och varför personuppgifter samlas in och hur personuppgifterna sedan används. De registrerade ska också få information om sina rättigheter, så som rätten att begära registerutdrag eller få uppgifter rättade (se avsnitt 8).

6.2. Ändamål med personuppgiftsbehandlingen

6.2.1. Ändamålsbegränsning

Personuppgifter får bara samlas in för särskilt uttryckligt angivna och berättigade ändamål, dvs. det finns en ändamålsbegränsning. Ändamålet ska vara fastställt och dokumenterat i GDPR Hero innan vi påbörjar behandlingen. Denna dokumentering är ett krav för att kunna visa att principen om ansvarsskyldighet är uppfylld (se avsnitt 6.7).

Ändamålen måste vara specifika och konkreta, dvs. de får inte vara luddiga eller otydliga. Skriv ändamålet så att såväl verksamheten som den registrerade kan förstå vad behandlingen faktiskt innebär.

Ändamålet måste också vara berättigat. Detta innebär att personuppgiftsbehandlingen dels ska ha en rättslig grund i dataskyddsförordningen, dels ska ske i enlighet med övrig tillämplig lagstiftning och allmänna rättsprinciper.

6.2.2. Behandling av personuppgifter i nya sammanhang (för nya ändamål)

Om det blir aktuellt med en behandling av personuppgifter i ett sammanhang som inte var planerat från början och som innebär att behandlingen sker för nya ändamål så ska den enhet/verksamhet som vill påbörja den nya behandlingen alltid utvärdera och dokumentera behandlingen i GDPR Hero. Detta ska ni göra innan ni påbörjar behandlingen för att säkerställa att den inte innebär en integritetskränkning för de registrerade samt att den inte bryter mot dataskyddsförordningen eller annan tillämplig lagstiftning.

Diskutera alltid ske med verksamhetens personuppgiftssamordnare innan ni påbörjar behandlingen. Vid osäkerhet kan ni alltid inhämta råd från dataskyddsombudet.

6.3. Uppgiftsminimering

Personuppgifter som verksamheten behandlar ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet. Det innebär att vid varje personuppgiftsbehandling så ska verksamheten säkerställa att vi inte samlar in fler personuppgifter än vad vi behöver för det aktuella ändamålet. Verksamheten (gäller ner på medarbetarnivå) får aldrig samla in personuppgifter för att de ”kanske kan vara bra att ha”.

De ställningstaganden och rutiner rörande hur respektive del av verksamheten arbetar för att leva upp till kraven om uppgiftsminimering ska finnas dokumenterat i GDPR Hero.

6.4. Riktighet

Personuppgifterna ska vara riktiga och om nödvändigt uppdaterade. Om personuppgifterna är felaktiga ska vi genomföra åtgärder för att rätta eller radera dem.

6.5. Lagringsminimering

Personuppgifter som inte längre behövs med hänsyn till ändamålet (och som vi inte heller är skyldig att spara) ska gallras i enlighet med verksamhetens dokumenthanteringsplan. Observera att det kan finnas lagkrav på att arkivera och spara uppgifter, vilket även ska framgå av dokumenthanteringsplanen.

Personuppgifter får inte användas på annat sätt, överföras till eller behandlas på annan plats (system/lagringsställe/enhet) än vad som följer av gällande rutiner och instruktioner.

Varje ny personuppgiftsbehandling ska anmälas till verksamhetens personuppgiftssamordnare, som för in den i registerförteckningen samt säkerställer att dokumenthanteringsplanen blir uppdaterad.

6.6. Lämplig säkerhet och informationssäkerhet

6.6.1. Lämplig säkerhet och exempel på säkerhetsåtgärder

Vid behandling av personuppgifter ska verksamheten leva upp till principen om integritet och konfidentialitet genom lämpliga tekniska och organisatoriska säkerhetsåtgärder, för att säkerställa att säkerhetsnivån är lämplig i förhållande till den risk som finns. Vid bedömning av vilken säkerhetsnivå som är lämplig ska beaktas den senaste utvecklingen, kostnader för genomförandet, behandlingens art, i vilken omfattning behandlingen sker (hur många personer som behandlingen omfattar samt hur ofta den sker), vilket ändamål som finns samt vilka risker som finns.

Exempel på säkerhetsåtgärder är

- pseudonymisering och kryptering av personuppgifter
- förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos systemen
- förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident
- ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet
- låsutrustning
- inpasseringskontroll
- larmutrustning för till exempel rök, brand, vatten och inbrott
- utrustning som skyddar vid strömavbrott eller strömstörningar
- säkerhetsskåp
- behörighetskontroll
- behandlingshistorik (loggning)
- inloggning och lösenord
- rutiner vid besök
- rutiner vid distansarbete

6.6.2. Inbyggt dataskydd och dataskydd som standard

Inbyggt dataskydd (privacy by design) innebär att hänsyn tas till de registrerades integritet redan vid utformning av IT-system och rutiner.

Dataskydd som standard ska tillgodoses genom att personuppgifter inte ska behandlas i onödan (exempelvis genom att inte mer information än nödvändigt samlas in, delas ut eller visas).

Detta kan uppnås genom i huvudsak följande åtgärder

- Minimera mängden personuppgifter i systemen genom att exempelvis när de registrerade ska lämna uppgifter endast ha fält för de personuppgifter som är nödvändiga för ändamålet. Undvik fritextfält och i de fall de behövs så bör en påminnelse till den registrerade finnas att vara integritetsmedveten när denne för in personuppgifterna.
- Begränsa åtkomsten till uppgifterna genom behörighetsstyrning.
- Säkra autentiseringar genom flerfaktorsinloggningar.
- Skapa krypteringsfunktioner.
- Skapa säkrare fysiska enheter (t.ex. telefoner, datorer, servrar).
- Genomföra utbildningar.
- Pseudonymisering.

Förbundet ska sträva efter att skapa ett inbyggt dataskydd i alla system och ha dataskydd som standard, så att systemen, tjänsterna och rutinerna kan uppfylla personuppgiftsansvarigs säkerhetskrav. Detta innebär att principen om inbyggt dataskydd och möjligheten att ha dataskydd som standard alltid bör beaktas vid inköp och upphandling och under hela IT-systemets livscykel (se avsnitt 5, rubrik Upphandlare).

6.6.3. Behörighetsbegränsning

Varje verksamhetsgren ska genom interna rutiner säkerställa att de medarbetare som har tillgång till personuppgifter har behov av dem i sitt arbete genom att ha en behörighetsbegränsning i t.ex. verksamhetssystem, gemensamma kataloger (G:) etc.

Förekommer känsliga personuppgifter ska behörighetsbegränsningen vara snävare än vad som gäller generellt sett inom verksamheten när behandling sker av mer harmlösa personuppgifter. Närmaste chef ska säkerställa att rätt behörigheter tilldelas rätt personer.

6.6.4. Riskanalys

Alla personuppgifter ska skyddas genom lämpliga säkerhetsåtgärder. Bedömningen om vilka säkerhetsåtgärder som är aktuella för en eller flera personuppgiftsbehandlingar avgörs genom att en riskbedömning genomförs och dokumenteras i diariet. En riskanalys ska alltid genomföras innan en ny behandling av personuppgifter påbörjas. Checklista för riskanalys finns i bilaga 2.

Om det vid riskbedömningen framkommer att behandlingen innebär en hög risk för de registrerades fri- och rättigheter, ska även en konsekvensbedömning genomföras.

Vid riskanalysen ska ni bedöma själva risken, dvs. beskriva

- händelsen och varför den kan vara en potentiell risk
- hur sannolikt det är att händelsen inträffar
- hur allvarliga konsekvenserna blir om händelsen inträffar.

Det kan exempelvis vara en hög risk om det saknas tillräckliga säkerhetsåtgärder så att obehöriga personer kan få ta del av personlig eller känsliga personuppgifter.

Rådgör med personuppgiftssamordnare eller dataskyddsombudet vid oklarheter. Kom ihåg att alltid dokumentera, motivera och omvärdera en riskanalys. Om förhållandena ändras kan det vara aktuellt att göra en ny riskanalys.

6.6.5. Konsekvensbedömning

Om en personuppgiftsbehandling innebär en hög risk för de registrerades fri- och rättigheter ska en konsekvensbedömning genomföras innan behandlingen påbörjas. Påbörja gärna konsekvensbedömningen så tidigt som det är praktiskt möjligt. En konsekvensbedömning kan genomföras för en enda behandling eller flera liknande behandlingar (om de liknar varandra vad gäller *art, omfattning, innehåll, ändamål och risker*). Checklista för konsekvensbedömning finns i bilaga 3.

Överväg alltid att göra en konsekvensbedömning i följande fall

- Vid upphandling och inköp av system, program, tjänster och/eller applikationer som behandlar känsliga eller extra skyddsvärda personuppgifter.
- Användning av ny teknik.
- Många användare kan ta del av personuppgifterna.
- Behandlingen avser ett stort antal personer eller en stor mängd personuppgifter.
- Behandlingen sker via öppna nätverk såsom Internet.

<u>Grundläggande krav vid en konsekvensbedömning</u>

- En systematisk beskrivning av den planerade behandlingen och behandlingens syfte.
- En bedömning av om behandlingen är nödvändig och proportionerlig i förhållande till syftet med den.
- En bedömning av riskerna för de registrerades rättigheter och friheter.
- Planerade åtgärder för att hantera risker och för att visa att kraven i dataskyddsförordningen är uppfyllda.

Dessutom bör ni rådgöra med dataskyddsombudet. I de fall det är lämpligt bör ni även hämta in synpunkter från de registrerade. När konsekvensbedömningen är klar så överväg om den ska publiceras, något som kan hjälpa till att uppfylla principerna öppenhet och ansvarsskyldigheten i dataskyddsförordningen.

<u>Avhjälpa risker</u>

Överväg i första hand om personuppgiftsbehandlingen är nödvändig och proportionerlig i förhållande till syftet. Kanske kan syftet med behandlingen uppnås på ett annat sätt så att riskerna inte uppstår. Exempel på åtgärder som kan användas för att hantera eller minska riskerna med en behandling finns i avsnitt 6.6.1.

Ompröva riskbedömningen kontinuerligt
Konsekvensbedömningen är en ständigt pågående process och avslutas inte med att den har blivit färdigställd. Utan vi måste utvärdera den med jämna mellanrum, detta beror på att behandlingen kan ha ändrats så att vi måste göra en ny konsekvensbedömning eller göra en bedömning om det inte tidigare har gjorts någon. Vid en ny bedömning så ska även denna dokumenteras, oavsett om bedömningen resulterar i att vi ska göra en ny konsekvensbedömning eller inte.

När ska tillsynsmyndigheten tillfrågas (förhandssamråd)?
Om det efter att en konsekvensbedömning är genomförd fortfarande kvarstår en hög risk ska personuppgiftsansvarig kontakta tillsynsmyndigheten för samråd innan behandlingen påbörjas.

När krävs inte en konsekvensbedömning?
Det krävs inte en konsekvensbedömning om:

- Behandlingen INTE ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.”
- Behandlingen är mycket lik en annan behandling där vi redan genomfört en konsekvensbedömning, där liknelsen rör behandlingens art, omfattning, sammanhang och ändamål.
- Behandlingen har en rättslig grund i förordningar eller i lag och om en allmän konsekvensbedömningen redan är genomförd i samband med antagandet av denna rättsliga grund.

6.6.6. Informationssäkerhet
Personuppgifter är en del av den information som behandlas inom verksamheten. Hur behandlingen ska ske utifrån IT- och informationssäkerhet framgår av förbundets strategi för informationssäkerhet samt riktlinje för informationssäkerhet.

6.7 Ansvarsskyldighet
Personuppgiftsansvarig ansvarar för att all personuppgiftsbehandling inom verksamheten följer de grundläggande principerna i dataskyddsförordningen. Personuppgiftsansvarig ska även kunna visa att de följs samt på vilket sätt. Det är därför mycket viktigt att vi följer strategi och riktlinje för behandling av personuppgifter och därmed t.ex. dokumenterar vårt arbete med behandling av personuppgifter (exempelvis vilka säkerhetsåtgärder som finns vid en personuppgiftsbehandling, vilka ändamål en personuppgiftsbehandling har etc).

7. Personuppgifter som är känsliga, extra skyddsvärda, mycket personliga eller skyddade inom folkbokföringen

7.1. Känsliga personuppgifter
Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd. De kallas för känsliga personuppgifter och är uppgifter om

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse

- medlemskap i fackförening
- hälsouppgifter *(fysisk eller psykisk hälsa exempelvis uppgifter från tester, om sjukdom, sjukdomsrisk, sjukdomshistoria, funktionshinder)*
- en fysisk persons sexualliv eller sexuella läggning
- genetiska uppgifter *(alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken, vilket ger unik information om personens fysiologi eller hälsa, är ofta en analys av ett biologiskt prov från personen i fråga)*
- biometriska uppgifter för att entydigt identifiera en fysisk person *(exempelvis ansiktsbilder och fingeravtrycksuppgifter)*.

Huvudregeln är att det är förbjudet att behandla känsliga personuppgifter, men det finns undantag i dataskyddsförordningen. Identifiera och dokumentera vilket undantag som är tillämpligt innan behandling av känsliga personuppgifter påbörjas. Tänk på att det kan finnas undantag i unionsrätt eller nationell rätt som medför att undantaget inte är tillämpbart i det enskilda fallet. Dokumentationen ska diarieföras i diariet.

Nedan finns exempel på undantag för att få behandla känsliga personuppgifter.
OBS! E*xemplen är endast översiktligt beskrivna, se artikel 9 i dataskyddsförordningen för samtliga undantag samt en fullständig beskrivning.*

- Samtycke från den registrerade.
- Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd. Exempelvis så ska en arbetsgivare betala ut sjuklön.
- Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke. Kan exempelvis vara aktuellt om den registrerade plötsligt blir sjuk och medvetslös för att kunna ta reda på sjukdomshistorik eller kontakta anhöriga.
- Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.
- Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk. Exempelvis behandling av etniskt ursprung inom skolan för att eleven har rätt att få modersmålsundervisning.
- Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse. Ett exempel på ett viktigt allmänt intresse är den grundlagsfästa rätten att ta del av allmänna handlingar.
- Behandlingen är nödvändig för arkivändamål av exempelvis allmänt intresse.

I vissa fall räcker det inte att titta i dataskyddsförordningen för att hitta undantag mot förbudet mot att behandla känsliga personuppgifter utan det kan krävas stöd i svensk eller europeisk lagstiftning eller i kollektivavtal. Den kompletterande dataskyddslagen innehåller till exempel några generella bestämmelser som gör det möjligt att behandla känsliga personuppgifter.

Känsliga personuppgifter ska inte skickas, varken internt eller externt, med okrypterad e-post. Personuppgifter som är känsliga ska istället skickas i ett förslutet kuvert. För att säkerställa att kuvertet inte har öppnats innan det når mottagaren bör sekretesstejp användas över tejpförslutningen på kuvertet. Kuvertet placeras i en internpost-mapp (internt) eller i ett ytterkuvert (utomstående mottagare). Som alternativ till att vidarebefordra internt i ett förslutet kuvert kan behörighetsbegränsade mappar på den gemensamma katalogen (G:) användas under förutsättning att inga obehöriga kan öppna mappen, att mappen inte ligger i Molnet, samt att informationssäkerhetssamordnaren och dataskyddsombudet godkänt den aktuella lösningen.

7.2. Extra skyddsvärda personuppgifter

Det finns personuppgifter som är extra skyddsvärda (även kallade särskilt skyddsvärda eller integritetskänsliga) personuppgifter. Om personuppgifterna är extra skyddsvärda kan det krävas att säkerhetsnivån vid personuppgiftsbehandlingen är högre än för mer harmlösa personuppgifter. Det kan även påverka bedömningen vid en konsekvensbedömning eller vid bedömningen om en personuppgiftsincident ska rapporteras till tillsynsmyndigheten eller inte.

Exempel (kan finnas fler) på extra skyddsvärda personuppgifter är

- personnummer och samordningsnummer
- löneuppgifter
- uppgifter om lagöverträdelser
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler
- information som rör någons privata sfär
- uppgifter om sociala förhållanden.

7.3. Personuppgifter av mycket personlig karaktär

Vissa personuppgifter kan vara av mycket personlig karaktär. Vid behandling av dessa personuppgifter kan vi t.ex. behöva göra en konsekvensbedömning inför vår behandling.

Exempel på personuppgifter av mycket personlig karaktär

- Uppgifter om hushållet och privat verksamhet, till exempel elektronisk kommunikation.
- Uppgifter som påverkar utövandet av en grundläggande rättighet, till exempel lokaliseringsuppgifter som kan göra att den fria rörligheten ifrågasätts.
- Finansiella uppgifter som skulle kunna användas för betalningsbedrägeri.
- Uppgifter såsom personliga dokument, e-postmeddelanden, dagböcker, kommentarer från läsplattor som är utrustade med kommentarfunktioner och mycket personlig information i applikationer som registrerar aktiviteter.

7.4 Skyddade personuppgifter (inom folkbokföringen)

Som huvudregel är uppgifter inom folkbokföringsverksamheten offentliga, men det finns undantag när den registrerade kan skadas om uppgifterna lämnas ut t.ex. om denne är hotad eller förföljd. Skyddade personuppgifter är det samlingsnamn som ofta används för de olika skyddsåtgärderna som finns rörande folkbokföringsuppgifter som är

markering av skyddade personuppgifter, kvarskrivning och fingerade personuppgifter. Alla dessa skyddsåtgärder kan vara kombinerade med tex. namnbyte.

Vi får uppgift från Skatteverket genom folkbokföringsdatabasen när dessa sekretessmarkeringar föreligger. Eftersom det inte åligger oss att utan anledning kontrollera sekretessmarkeringar i folkbokföringen så finns även ett ansvar för den registrerade att upplysa om en eventuell sekretessmarkering.

Det är viktigt att hantera personer med skyddade personuppgifter med stor aktsamhet, varför det även är viktigt att tänka igenom vilka som ska vara inblandade i ärenden som rör personer med skyddade personuppgifter. Varje verksamhetsdel ska ha särskilt utsedda medarbetare som behandlar skyddade personuppgifter.

7.4.1. Generella instruktioner vid hantering av skyddade personuppgifter

- All dokumentation ska vara skyddad på ett säkert sätt så att den inte röjs.
- All utskriven dokumentation t.ex. en pappersakt ska förvaras i låsta utrymmen där endast särskilt utsedda personer har åtgång.
- Om den skyddade uppgiften (ej personnummer) finns dokumenterad sedan tidigare då den inte var skyddad, ska uppgiften markeras och inte användas (trots personens samtycke). Om det inte är möjligt att markera uppgiften ska uppgiften döljas eller sparas på annan säker plats.
- Personuppgifter som finns i något system som många har tillgång till, t.ex. planeringssystem, och som blir skyddade, ska plockas bort manuellt. Om uppgifterna ska sparas förvaras de i en pappersakt i låst utrymme.
- Ta inte med formaliainformation t.ex. adressuppgifter och telefonnummer i handlingar i onödan.
- Använd säkra kommunikationskanaler såsom brev (via Skatteverkets förmedlingstjänst), elektronisk kommunikation med hjälp av e-legitimation och personligt besök.
- Prata aldrig om en person med skyddade personuppgifter annat än med berörda medarbetare i enrum.
- Upprätta anpassade rutiner för varje person med skyddade personuppgifter och utse medarbetare som den registrerade har kontakt med i första hand. De anpassade rutinerna kan t.ex. innebära att skolan eller förskolan kommer överens med vårdnadshavaren hur barnets personuppgifter ska hanteras i skolan exempelvis klasslistor, skolkataloger, sjukanmälan, utflykter, vem som ska kontaktas om något inträffar, hur vi ska svara om någon ringer eller kommer till skolan/arbetsplatsen och efterfrågar personen m.m.
- Personer med skyddade personuppgifter ska som huvudregel inte finnas med på listor t.ex. klasslistor (om inte samtycke finns från den registrerade eller dennes vårdnadshavare).
- Personer med skyddade personuppgifter ska inte finnas med på foton t.ex. skolfoton, foton som beskriver kommunens verksamhet etc om det inte finns ett samtycke (godkännande) från den registrerade eller dennes vårdnadshavare.
- ###förvaltningschef? ger behörighet till de fåtal personer som ska ha behörighet till personuppgifterna och systemansvarig administrerar uppgiften.

- Håll dig uppdaterad om din verksamhets rutiner för hantering av skyddade personuppgifter.

Skicka post till någon med skyddade personuppgifter

1. Lägg brevet som ska förmedlas i ett kuvert.
2. Skriv personens personnummer och namn (om du känner till det) på kuvertet.
3. Klistra igen kuvert och skriv avsändare på baksidan.
4. Lägg kuvertet i ett ytterkuvert och adressera till Skatteverkets förmedlingsadress på det yttre kuvertet (om inte Skatteverket aviserat en annan adress i det enskilda fallet):
   Skatteverkets förmedlingsuppdrag
   Box 2820
   40320 Göteborg

7.4.1. Skyddad folkbokföring (har ersatt kvarskrivning)

Skyddad folkbokföring innebär att den registrerade är folkbokförd på en annan folkbokföringsort än hen är bosatt. De som tidigare hade kvarskrivning har sedan 1 januari 2019 skyddad folkbokföring. Personer med skyddad folkbokföring är folkbokförda ”på kommunen” vilket antingen är en kommun som personen flyttat ifrån eller i en annan kommun som det inte finns någon anknytning till. Den registrerade får sin post till Skatteverket.

7.4.2. Sekretessmarkering i folkbokföringen

Skatteverket kan registrera en sekretessmarkering i folkbokföringsdatabasen under vissa förutsättningar. Sekretessmarkeringen är en varningssignal att det finns behov av att vi gör en noggrann skadeprövning när någon begär att få ut en sekretessmarkerad uppgift. Sekretessmarkeringen är innebär ingen absolut sekretess, utan är en administrativ åtgärd liknade hemligstämpeln på ett dokument.

7.4.3. Fingerade personuppgifter

Fingerade personuppgifter innebär att en person blir registrerad i folkbokföringen med andra personuppgifter än de verkliga. Någon koppling mellan de gamla och nya uppgifterna finns inte. Uppgifterna som registreras hos Skatteverket så att sambandet mellan de verkliga och de fingerade inte framgår.

8. De registrerades rättigheter

De registrerade har ett antal rättigheter enligt dataskyddsförordningen. Dessa rättigheter innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas och kunna ha kontroll över sina egna uppgifter. Därför finns även möjlighet till att i vissa fall få uppgifterna rättade, raderade eller blockerade.

<u>Identifiering av de registrerade</u>

När en registrerad begär någon form av åtgärd avseende personuppgifter måste identifiering ske för att säkerställa att det är rätt person som begär åtgärden. Om inte identifiering kan ske elektroniskt i t.ex. en e-tjänst så kan den registrerade exempelvis komma till receptionen och identifiera sig med godkänd legitimationshandling.

8.1. Information till de registrerade

Alla vars personuppgifter vi behandlar har rätt att känna till varför vi behandlar deras personuppgifter samt vilka ändamålen är. Informationen ska vara skriven med klart och tydligt språk, vara lättillgänglig samt tillräckligt utförlig för att motsvara de krav som finns i dataskyddsförordningen. Tänk på att alltid rikta informationen till målgruppen, t.ex. barn. När det gäller barn så tänk på barnperspektivet för att säkerställa att de förstår sina rättigheter och vad behandlingen avser. Informationen till barn ska vara särskilt enkel att förstå.

De registrerade ska få information om behandlingen när vi samlar in personuppgifterna, om den registrerade inte redan förfogar över uppgifterna. Information ska även lämnas till en registrerad om denne begär att få informationen genom ett s.k. registerutdrag.

Eftersom informationen ska lämnas när vi samlar in personuppgifterna ska den finnas i våra e-tjänster samt på våra blanketter så att vi säkerställer att de registrerade kan ta del av den i samband med vår insamling. Informationen vid varje e-tjänst eller blankett ska beskriva just den aktuella behandlingen av personuppgifter och ska inte vara generellt skriven.

I de fall insamlingen sker från annan än den registrerade eller på annat sätt än genom en e-tjänst eller blankett så ska information överlämnas till den registrerade så snart som möjligt.

Utöver den specifika informationen vid en viss personuppgiftsinsamling ska vi ha generell information om verksamhetens behandling av personuppgifter, de registrerades rättigheter samt kontaktuppgifter till personuppgiftsansvarig och dataskyddsombud på vår webbplats samt på vårt intranät.

8.2. Information när den registrerade begär, s.k. registerutdrag

Den registrerade har rätt att få bekräftelse på om personuppgifter som rör honom eller henne behandlas och i sådana fall få tillgång till personuppgifterna. Informationen ska vara lättillgänglig, skriftlig och skriven på ett tydligt och enkelt språk. Om vi tar emot ansökan elektroniskt ska vi även tillhandahålla registerutdraget elektroniskt om den registrerade inte begär annat. Säkerställ att rätt person begär registerutdrag samt om denne vill ha informationen muntligt så måste säkerställande även ske då.

Registerutdraget ska som huvudregel lämnas inom en månad från att vi mottagit begäran. Tiden kan förlängas med ytterligare två månader t.ex. om begäran är komplicerad eller om vi fått in många begäranden. Vid förlängning av tiden ska den registrerade alltid få information om förseningen inom den första månaden.

Tänk på att inte ta med uppgifter som omfattas av sekretess mot den registrerade själv eller om en vårdnadshavare begär registerutdrag för ett barn så ska utdraget inte innehålla uppgifter som omfattas av sekretess gentemot vårdnadshavaren.

Undantag från rätten att få registerutdrag (exempel

- Om begäran är ogrundad eller orimlig t.ex. man begär registerutdrag på registerutdrag (alternativt ta ut en avgift om en sådan finns beslutad inom verksamheten).
- Om det är sekretess gentemot den registrerade.
- Om det framgår av särskilda registerförfattningar att vissa personuppgifter inte får lämnas ut.
- Om det är personuppgifter i löpande text som inte har fått sin slutliga utformning när begäran gjordes eller som utgör minnesanteckning eller liknande (jfr 5 kap. 2 § dataskyddslagen). Undantaget i sig är dock inte tillämpligt om personuppgifterna (någon av alternativen föreligger)
    1. har lämnats ut till tredje part,
    2. behandlas enbart för arkivändamål av allmänt intresse eller statistiska ändamål,
    3. har behandlats under längre tid än ett år i löpande text som inte har fått sin slutliga utformning. (i 5 kap. 2 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, dataskyddslagen).

8.3. Rätt till rättelse

Varje person har rätt att vända sig till personuppgiftsansvarig och be att få felaktiga uppgifter rättade. Detta innebär också att den enskilde har rätt att komplettera med sådana personuppgifter som saknas och som är relevanta med hänsyn till ändamålet med personuppgiftsbehandlingen. Uppgifterna kan rättas eller kompletteras om de är felaktiga eller ofullständiga.

8.4. Rätt till radering (rätten att bli bortglömd)

Varje person har rätt att vända sig till personuppgiftsansvarig och be att uppgifter som avser denne raderas. Uppgifterna måste då raderas i vissa fall t.ex. de inte längre är nödvändiga i sitt sammanhang eller om det inte finns något berättigat skäl att behandla uppgifterna exempelvis om behandlingen grundar sig på ett samtycke som nu är återkallat.

Det finns dock undantag från rätten till radering såsom att bevarandet av personuppgifterna är nödvändigt för att tillgodose andra viktiga rättigheter som till exempel rätten till yttrande- och informationsfrihet, för att uppfylla en rättslig förpliktelse, utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning. Uppgifterna ska inte raderas om de ska finnas kvar enligt ett annat regelverk (exempelvis arkivlagstiftningen).

Personuppgiftsansvarig ansvarar för att säkerställa att det finns tydliga dokumenthanteringsplaner där det framgår när personuppgifter ska gallras inom det aktuella verksamhetsområdet.

8.5. Rätt att invända mot och begära begränsning av behandlingen

Den registrerade har rätt att göra invändningar mot behandlingen av personuppgifter, varpå vi då måste utreda om vi har skäl att fortsätta med vår behandling eller om den måste upphöra.

Enskilda har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas. Begränsning av behandling kan ske exempelvis genom att personuppgifter markeras så att de i framtiden endast kan behandlas för vissa avgränsade syften.

8.6. Dataportabilitet

Om den lagliga grunden är samtycke eller avtal och behandlingen sker automatiserat så har den registrerade rätt till dataportabilitet när detta är tekniskt möjligt. Dataportabilitet innebär att personuppgifterna överförs från en personuppgiftsansvarig till en annan.

8.7. Synpunkter och klagomål

Synpunkter eller klagomål på vår behandling kan framföras till respektive personuppgiftsansvarig eller till verksamhetens dataskyddsombud.

Den registrerade har även möjlighet att lämna in synpunkter eller klagomål direkt till tillsynsmyndigheten, något vi alltid ska upplysa om i vår information till den registrerade.

9. Dokumentation, gallring, arkivering

Det är viktigt att vi dokumenterar vilka åtgärder vi genomför i vårt arbete med att uppfylla kraven i dataskyddsförordningen. Exempel på handlingar som rör behandling av personuppgifter och som alltid ska diarieföras är

- ✓ Handlingsplaner
- ✓ Åtgärdsplaner
- ✓ Beslut att utse dataskyddsombud
- ✓ Handlingar till och från tillsynsmyndigheten (exempelvis personuppgiftsincidenter, samråd, kontaktuppgifter till dataskyddsombudet)
- ✓ Personuppgiftsbiträdesavtal eller andra rättsakter vid biträdessituationer
- ✓ Förteckning över inhämtade och ej gallrade samtycken
- ✓ Riskanalyser
- ✓ Konsekvensbedömningar
- ✓ Personuppgiftsincidenter

Respektive personuppgiftsansvarigs verksamhets dokumenthanteringsplaner ska reglera vad som gäller för gallring och arkivering.

10. Personuppgifter i e-post, kallelser, protokoll och webbplats

10.1. Personuppgifter i e-post

Vi ska inte skicka känsliga eller extra skyddsvärda personuppgifter via e-post. Om det är absolut nödvändigt att använda sig av e-post för dessa personuppgifter så måste det finnas kryptering.

Om vi får in känsliga personuppgifter via e-post så bör uppgifterna överföras till ett lämpligare system (exempelvis ett ärendehanteringssystem eller en behörighetsstyrd gemensam mapp på G:), om vi har en rättslig grund för att spara uppgifterna). E-postmeddelandet ska därefter raderas.

E-post som vi mottar blir normalt en allmän handling som ska registreras eller hållas ordnad. Vi skyldiga att bevara allmänna handlingar enligt arkivlagen. Utgångspunkten är därför att det är tillåtet för oss att bevara handlingarna för att uppfylla kraven i arkivlagen.

10.2. Publicering av personuppgifter i kallelse, protokoll och webbplats

Personuppgifter avseende tjänstepersoner och förtroendevalda politiker som har anknytning till deras tjänsteutövning eller uppdrag får behandlas i kallelser, protokoll och på webbplatsen.

Personuppgifter i kallelser till förtroendevalda politiker samt tjänstepersoner som är kallade till sammanträdet får innehålla personuppgifter, om dessa inte är sekretessbelagda. Sekretessbelagda uppgifter finns att läsa på kansliet.

Om personuppgifter avseende enskilda personer finns i handlingar som ska publiceras ska dessa maskas innan publicering. Känsliga eller extra skyddsvärda personuppgifter ska aldrig finnas med vid publicering.

Sekretessbelagd information ska aldrig publiceras på kommunens webbplats (t.ex. på anslagstavlan).

I anknytning till anslagstavlan ska det finnas ett förtydligande i form av t.ex. ”Vi publicerar inte vissa personuppgifter eller handlingar på webbplatsen med anledning av dataskyddsförordningen eller sekretesslagstiftningen. Önskar du ta del av allmänna handlingar så är du välkomna att kontakta oss.”.

11. Förteckning över behandlingar (registerförteckning)

Varje personuppgiftsansvarig och, i tillämpliga fall, dennes företrädare ska föra ett register över de personuppgiftsbehandlingar som utförts under dess ansvar. Registret kallas ofta regiterförteckning.

Även om det inte är en systemförteckning så bör det även framgå i vilka system som behandlingen förekommer, vilket exempelvis underlättar utredningen vid en personuppgiftsincident.

<u>Registerförteckningen ska vara</u>

- skriftlig
- elektronisk
- uppdaterad

<u>Registerförteckningen ska innehålla följande information för varje behandling</u>

- Namn och kontaktuppgifter för den personuppgiftsansvarige (direktionen), samt i tillämpliga fall gemensamt personuppgiftsansvariga, den personuppgiftsansvariges företrädare samt dataskyddsombud.
- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade (exempelvis elever, anställda, vårdnadshavare) och av kategorierna av personuppgifter (exempelvis namn, personnummer, adress).

- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, inbegripet mottagare i tredjeländer eller i internationella organisationer.
- Vid överföringar av personuppgifter till ett tredjeland (utanför EU/EES) eller en internationell organisation ska det framgå till vilket land/organisation samt finnas en dokumentation av vilka lämpliga skyddsåtgärder som genomförts.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter. Se dokumenthanteringsplanen.
- En allmän beskrivning av de tekniska och organisatoriska säkerhetsåtgärderna (se artikel 32.1. i dataskyddsförordningen).

Varje verksamhetsdel ska anmäla in de behandlingar som finns i verksamheten till personuppgiftssamordnaren som registrerar dessa i registerförteckningen.

12. Personuppgiftsbiträden och biträdesavtal

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation, vilket innebär att anställda aldrig är att anse som ett biträde. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

Det ska finnas skriftliga biträdesavtal (eller en annan rättsakt) med samtliga leverantörer och andra personuppgiftsbiträden. I första hand ska personuppgiftsbiträdesavtal finnas med redan i upphandlingsdokumenten. I de fall det inte finns så ansvarar avdelningschef/annan utsedd person för att se till att ett personuppgiftsbiträdesavtal finns tecknat och diarieført med huvudavtalet.

Vi använder oss som huvudregel av Sveriges Kommuner och Regioners senaste version till personuppgiftsbiträdesavtal. Om ett annat avtal väljs så måste avdelningschef/annan utsedd person säkerställa att avtalet uppfyller kraven i artikel 28 i dataskyddsförordningen samt verksamhetens krav på t.ex. informationssäkerhet.

Har du som ska teckna personuppgiftsbiträdesavtal någon fråga du vill diskutera rörande avtalet kan du vända dig till verksamhetens personuppgiftssamordnare. Kan denne inte besvara dina frågor kan ni alltid vända er till dataskyddsombudet.

13. Gemensamt personuppgiftsansvar

Om flera personuppgiftsansvariga gemensamt bestämmer över en personuppgiftsbehandling så är de även gemensamt personuppgiftsansvariga för den aktuella behandlingen. Detta innebär att man i praktiken behöver avtala om vem av de ansvariga som ska fullgöra de olika skyldigheterna som personuppgiftsansvarig har enligt dataskyddsförordningen. Avtalet ska ge svar på vilka respektive roller parterna har och det ska finnas tillgängligt för de registrerade. Oavsett vad avtalet innebär så kan de registrerade dock utöva sina rättigheter gentemot var och en av de personuppgiftsansvariga.

Det är respektive verksamhet som ska inventera sina behandlingar av personuppgifter för att se om det finns någon behandling som innebär ett gemensamt personuppgiftsansvar. I de fall det förekommer så ska ett gemensamt arrangemang i form av ett avtal tecknas mellan parterna och synliggöras för de registrerade (exempelvis i den information som lämnas när behandlingen påbörjas).

Avtalet ska efter det är undertecknat diarieföras med huvudavtalet.

14. Personuppgiftsincidenter

14.1. Vad är en personuppgiftsincident?

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för fysiska personers rättigheter och friheter, såsom exempelvis brott mot sekretess eller tystnadsplikt, finansiell förlust, diskriminering, identitetsstöld, bedrägeri eller skadlig ryktesspridning. En personuppgiftsincident har exempelvis inträffat om uppgifter som avser en eller flera registrerade personer har blivit förstörda, gått förlorade på annat sätt eller kommit i orätta händer, oavsett om det skett oavsiktligt eller med avsikt.

14.2. Anmäl personuppgiftsincidenter internt

Alla medarbetare och förtroendevalda politiker ansvarar för att anmäla en personuppgiftsincident direkt när incidenten upptäcks. Anmäl incidenten genom e-tjänsten i som du når via intranätet.

14.3. Personuppgiftssamordnare – att göra vid en incident

14.3.1. Ta emot och diarieför

Så snart du tagit emot anmälan om personuppgiftsincident ska du se till att den blir diarieförd. I diariet samlar du sedan samtlig information och dokumentation rörande personuppgiftsincidenten. Diarieföring ska även ske i de fall det inte är aktuellt att anmäla personuppgiftsincidenten till tillsynsmyndigheten.

14.3.2. Gå igenom och utred personuppgiftsincidenten

Gå igenom anmälan för att bilda dig en uppfattning av vilken slags incident det är och hur allvarlig den är.

Om den är IT-relaterad (IT-incidenter, förlorade datorer, telefoner, surfplattor etc.) kontrollerar du omgående om IT- och Teleenheten är kontaktade, i annat fall informerar du dem direkt.

Kontrollera att alla relevanta uppgifter som du behöver för din utredning är med i anmälan. Annars tar du kontakt med den som lämnat in anmälan (eller annan relevant

person) för att gå igenom vad som hänt samt vilka åtgärder som eventuellt redan har genomförts.

I bilaga 1 finns exempel på vad en personuppgiftsincident kan innebära, vad orsaken kan vara samt exempel på när en anmälan till tillsynsmyndigheten ska ske respektive inte ske.

Vid behov kan du kontakta tillsynsmyndigheten för att få information och råd.

Dokumentera alla dina kontakter och bedömningar och diarieför dem.

14.3.3. Är vi personuppgiftsbiträde?

Omfattar incidenten personuppgifter som vi behandlar i egenskap av personuppgiftsbiträde ska du omgående lämna information om incidenten till personuppgiftsansvarig. Finns inte all information så lämna skyndsamt den information som finns och komplettera sedan så fort det går.

Vad informationen ska innehålla framgår oftast av personuppgiftsbiträdesavtalet mellan parterna. Om det inte framgår i personuppgiftsbiträdesavtalet ska du informera om:

1. Personuppgiftsincidentens art och, om möjligt, de kategorier och antalet registrerade som berörs samt kategorier och antalet personuppgiftsposter som berörs,
2. Sannolika konsekvenserna av personuppgiftsincidenten,
3. Åtgärder som har genomförts eller föreslagits samt åtgärder för att mildra personuppgiftensincidentens potentiella negativa effekter
4. Namn och kontaktuppgifter på dataskyddsombud eller andra kontaktpunkter där mer information kan erhållas.

Det är alltid personuppgiftsansvarig som ska bedöma om incidenten ska anmälas till tillsynsmyndigheten, varför vi om vi endast är biträde inte ska ta ställning till detta.

Dokumentera och diarieför dina kontakter.

14.3.4. Information till de registrerade

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska personuppgiftsansvarig utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten. Om de registrerade inte fått någon information om incidenten gör du en bedömning om verksamheten ska lämna information eller inte. Du redogör sedan din bedömning för personuppgiftsansvarig

(eller av denne utsedd företrädare, nedan endast benämnt personuppgiftsansvarig) som i sin tur bestämmer om de registrerade ska informeras eller inte.

Om personuppgiftsansvarig anser att information ska lämnas till de registrerade ansvarar du i egenskap av personuppgiftssamordnare för att de registrerade får informationen skyndsamt.

Informationen till de registrerade ska innehålla följande:

- ✓ Beskriv orsaken till personuppgiftsincidenten klart och tydligt.
- ✓ Namn och kontaktuppgifter till dataskyddsombudet eller till en annan kontakt som är insatt i frågan och kan svara på frågor.
- ✓ Beskriv de sannolika konsekvenserna av personuppgiftsincidenten.
- ✓ Beskriv vad myndigheten har gjort, eller tänker göra, för att hantera personuppgiftsincidenten.
- ✓ I förkommande fall: Beskriv vad myndigheten har gjort för att mildra eventuella negativa effekter.

Dokumentera och diarieför såväl dina bedömningar som personuppgiftsansvarigs beslut, den information som eventuellt lämnats till de registrerade samt vilken tidpunkt informationen lämnades.

14.3.5. Kontakta dataskyddsombudet

Om du inte redan har varit i kontakt med dataskyddsombudet så kontakta gärna denne för att ha en dialog om incidenten om det inte är uppenbart att en anmälan ska ske alternativ inte ska ske. Oavsett vilket ska dataskyddsombudet alltid få information om inträffade personuppgiftsincidenter för kännedom, varför du åtminstone när incidenten är färdigutredd ska meddela denne.

14.3.6. Anmäla till tillsynsmyndigheten

Inom 72 timmar från att vi fick vetskap om personuppgiftsincidenten ska en eventuell anmälan till tillsynsmyndigheten ske via deras e-tjänst. Detta innebär att du måste utreda personuppgiftsincidenten skyndsamt. Anmälan ska ske inom denna tid även om utredningen inte är klar och behöver kompletteras, se avsnitt 14.3.7.

Gör en utredning och bedöm om det är osannolikt att personuppgiftsincidenten innebär risker för de registrerades fri- och rättigheter eller inte. Exempelvis att de förlorat kontrollen över sina uppgifter, att rättigheter inskränks, att de utsätts för diskriminering, identitetsstöld eller bedrägeri, finansiell förlust, skadlig ryktesspridning och brott mot sekretess eller tystnadsplikt. Se bilaga 1.

När din utredning är klar ska du överlämna utredningen samt ett förslag till beslut till personuppgiftsansvarig som i sin tur ska fatta ett beslut om anmälan ska ske till tillsynsmyndigheten eller inte. Av din utredning ska det framgå vad som hänt, vilka åtgärder vi genomfört (inklusive tidpunkter) samt om din bedömning är att en anmälan ska ske till tillsynsmyndigheten eller inte. Som personuppgiftssamordnare ska du diarieföra såväl din utredning och ditt förslag till beslut som personuppgiftsansvarigs beslut och själva anmälan om en sådan sker.

Om en anmälan ska ske så gör du den i tillsynsmyndighetens e-tjänst. Tänk på att all information i anmälan blir en allmän handling. Finns ingen sekretessregel kommer tillsynsmyndigheten efter en begäran lämna ut informationen. Undvik därför att lämna fler uppgifter än nödvändigt. Bedömer du att någon uppgift omfattas av sekretess så ange det i fritextfältet som finns sist i anmälan.

14.3.7. Komplettering till tillsynsmyndigheten

Finns inte all information som du och personuppgiftsansvarig behöver för att bedöma personuppgiftsincidenten inom 72 timmar så fortsätter du din utredning, underrättar personuppgiftsansvarig om vad utredningen visar samt kompletterar anmälan till tillsynsmyndigheten så fort den är klar.

14.3.8. Korrigerande åtgärder

Beroende på vad personuppgiftsincidenten innebar, så kan det vara aktuellt att fundera över om det krävs några korrigerande åtgärder i efterhand. Exempel på när det kan vara aktuellt med korrigerande åtgärder är om personuppgiftsincidenten innebär att det finns en brist i vår säkerhet eller om flera liknande personuppgifter har inträffat. De korrigerande åtgärderna kan vara att genomföra en riskanalys för att se vilka ytterligare säkerhetsåtgärder som behövs samt när de kan genomföras. Om flera liknande personuppgifter inträffat kan det vara aktuellt att skärpa riktlinjer eller kanske informera medarbetare och politiker hur man ska agera i de aktuella situationerna för att undvika framtida personuppgiftsincidenter.

Dokumentera och diarieför de korrigerande åtgärder som du föreslår. Överlämna till personuppgiftsansvarig som har att bestämma om åtgärderna kan och ska genomföras. Ditt förslag och personuppgiftsansvarigs ställningstagande ska dokumenteras och diarieföras.

14.3.9. Dokumentation

Du ska dokumentera och diarieföra samtliga utredningar, ställningstaganden, beslut, anmälningar till tillsynsmyndigheten etc. Dokumentationen möjliggör för verksamheten att i efterhand gå igenom vilka incidenter som inträffat, för dataskyddsombudet att

granska hur hanteringen av personuppgiftsincidenter skötts samt för tillsynsmyndigheten att kontrollera att personuppgiftsansvarig efterlever kraven i dataskyddsförordningen vid en incident.

14.4. Personuppgiftsansvarig – att göra vid en personuppgiftsincident

Personuppgiftsansvarig eller av denne utsedd företrädare (se delegationsordningen) ska anmäla en personuppgiftsincident till tillsynsmyndigheten inom 72 timmar efter att ha fått vetskap om den om det inte är osannolikt att den innebär en risk för de registrerades fri- och rättigheter.

Efter att ha fått ta del av personuppgiftssamordnarens utredning och förslag till beslut rörande personuppgiftsincidenten ska du besluta om du anser att det är osannolikt att personuppgiftsincidenten innebär en risk för de registrerades fri- och rättigheter eller inte. Om det inte är osannolikt ska du besluta att en anmälan ska ske.

I bilaga 1 finns exempel på vad en personuppgiftsincident kan innebära, vad orsaken kan vara samt exempel på när en anmälan till tillsynsmyndigheten ska ske respektive inte ske.

Om du beslutar att en anmälan ska ske så gör personuppgiftssamordnaren det genom att använda tillsynsmyndighetens e-tjänst.

I vissa fall finns inte tillräckligt med information inom 72 timmar, varför en anmälan kan behöva göras även på bristfälligt material för att sedan kompletteras.

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska personuppgiftsansvarig utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten. Mot bakgrund av dataskyddssamordnarens utredning beslutar du om de registrerade ska informeras eller inte.

Beroende på personuppgiftsincident kan det vara aktuellt med korrigerande åtgärder för att förhindra framtida liknande incidenter. Personuppgiftssamordnaren utreder detta och överlämnar till personuppgiftsansvarig för beslut. Men personuppgiftsansvarig kan såklart även själv bestämma om åtgärder även om de inte föreslagits. Förslag och beslut ska diarieföras.

Bilaga 1 Personuppgiftsincidenter

1. Exempel på personuppgiftsincidenter

Obehörigt röjande innebär att personuppgifter hanteras på ett sådant sätt att de kommer till obehörigas kännedom, t.ex. genom att personuppgifter avsiktligt eller oavsiktligt röjs för någon som saknar behörighet att ta del av dem eller om ett tekniskt fel medför att stora mängder personuppgifter kommer till fel mottagares kännedom. Ett exempel är felaktiga brevutskick eller e-postutskick, dvs. att fel mottagare får del av ett brev eller e-post innehållande personuppgifter.

Det krävs inte att någon faktiskt har tagit del av personuppgifterna för att det ska ha inträffat ett obehörigt röjande.

Obehörig åtkomst innebär att någon olovligen berett sig tillgång till personuppgifter. Ett exempel är om behörigheter till ett IT-system har tilldelats fel person eller för generellt. Att personuppgifter finns tillgängliga på gemensamma lagringsytor utan behörighetsstyrning är ett annat exempel. Det är alltid viktigt att ha skarpa krav på behörighetstilldelning i organisationen och rutiner och instruktioner för hur användarna får använda sina behörigheter samt möjlighet att kunna upptäcka om någon obehörig tar del av personuppgifter genom exempelvis loggning av system.

Även nätfiske s.k. phishing (bedragare som lurar internetanvändare att lämna ut känslig information) tillhör kategorin obehörig åtkomst.

Stöld och förlust av personuppgifter kan exempelvis handla om att en tjänstedator glömts i kollektivtrafiken, att verksamheten haft inbrott eller varit utsatta för ett angrepp genom till exempel skadlig kod (virus, trojaner etc.) eller hacking. En förlust av personuppgifter omfattar både när personuppgifter förstörs och när organisationen inte längre kan komma åt dem (men att de finns kvar) ett exempel är cyberattacker som låst informationen varefter organisationen fått betala för att kunna låsa upp dem.

Förstöring eller ändring av personuppgifter innebär att personuppgifter ändras, blivit korrumperade eller inte längre är kompletta. Det kan exempelvis ske om någon eller något har förstört informationen, till exempelvis om en dator som innehåller personuppgifter går sönder och uppgifterna inte finns sparade på annat sätt.

2. Vad är orsaken till personuppgiftsincidenten?

Den mänskliga faktorn. Personuppgiftsincidenter som beror på den mänskliga faktorn består i huvudsak av att individer i det enskilda fallet begått ett misstag vid hantering av personuppgifter i sina verksamheter. Det kan också handla om att individer, medvetet eller omedvetet, inte följer interna rutiner för hantering av personuppgifter. En vanlig incident som beror på mänskliga faktorn är felskickade brev och e-postmeddelanden.

Brist i organisatoriska rutiner eller processer innebär att de rutiner och processer som finns inte fungerat eller att de är otillräckliga och behöver revideras. Tillsynsmyndigheten tror att det finns ett stort mörkertal inom denna kategori, då flera av incidenterna sannolikt uppges bero på den mänskliga faktorn.

Tekniskt fel kan orsaka en personuppgiftsincident när det exempelvis är fel i mjukvaran eller en programinställning är felaktig. Ett exempel är om behörighetsbegränsningarna till ett IT-system förlorats vid en systemuppdatering.

Antagonistiska angrepp kan vara en phishingattack (nätfiske). Det kan även handla om att en medarbetare öppnat en länk eller en bifogad fil som innehåller exempelvis ett virus.

3. Exempel på när en personuppgiftsincident som huvudregel bör anmälas respektive inte anmälas till tillsynsmyndigheten

Exempel från tillsynsmyndighetens rapport över anmälda personuppgiftsincidenter januari – september 2019.			
Exempel	**Anmäla till tillsynsmyndighet?**	**Underrätta den registrerade?**	**Anmärkning / rekommendation**
1. Brev eller e-post sänds till fel person. Innehåller endast kontakt-uppgifter till en eller några få registrerade. Det finns ingen känslig information.	Nej.	Nej.	
2. Brev eller e-post sänds till fel person. Innehåller uppgifter om ett stort antal människor, finansiell information eller känsliga personuppgifter (exempelvis hälsouppgifter).	Ja.	Ja. Rapportera även till de berörda enskilda personerna beroende på personuppgifternas art och om det är sannolikt att de leder till mycket allvarliga konsekvenser för enskilda personer	

Exempel från Europeiska dataskyddsstyrelsen (European Data Protection Board, EDPB) riktlinjer om anmälan av personuppgiftsincidenter. Riktlinjen finner du här.			
Exempel	**Anmäla till tillsynsmyndighet?**	**Underrätta den registrerade?**	**Anmärkningar/ rekommendationer**
1. En personuppgiftsansvarig sparar en säkerhetskopia av ett arkiv över personuppgifter på ett USB-minne. Minnet stjäls under ett inbrott.	Nej.	Nej.	Så länge uppgifterna är krypterade med den senaste typen av algoritm, det finns säkerhetskopior av uppgifterna, det unika minnet inte har äventyrats och uppgifterna snabbt kan återställas, är det inte säkert att incidenten behöver rapporteras. Om uppgifterna senare äventyras krävs dock en anmälan.
2. En personuppgiftsansvarig driver en onlinetjänst. Till följd av ett it-angrepp på den tjänsten har enskilda personers personuppgifter exfiltrerats.	Ja, rapportera till tillsynsmyndigheten om incidenten sannolikt leder till konsekvenser för enskilda personer.	Ja, rapportera till enskilda personer beroende på de berörda personuppgifternas art och om det är sannolikt att de leder till mycket allvarliga konsekvenser för enskilda personer.	
3. Ett kort strömavbrott under några minuter på en personuppgiftsansvarigs teletjänstcentral innebär att kunder inte kan ringa till personuppgiftsansvarig och få tillgång till sina uppgifter.	Nej.	Nej.	Detta är inte en incident som behöver anmälas, men som trots det ska registreras enligt artikel 33.5. Den personuppgiftsansvarige bör föra ett lämpligt register.

4. En personuppgifts-ansvarig utsätts för ett angrepp med ransomware vilket leder till att alla uppgifter krypteras. Det finns inga säkerhetskopior och uppgifterna kan inte återställas. Vid en närmare undersökning visar det sig att det enda syftet med angreppet var att kryptera uppgifterna, och att det inte fanns några andra sabotageprogram i systemet.	Ja, rapportera till tillsyns-myndigheten om incidenten sannolikt leder till konsekvenser för enskilda personer eftersom detta utgör en förlust av tillgänglighet.	Ja, rapportera till enskilda personer, beroende på de berörda person-uppgifternas art och de potentiella konsekvenserna av förlusten av tillgänglighet, samt andra sannolika konsekvenser.	Om det fanns en säkerhetskopia och uppgifterna snabbt kunde återställas behöver incidenten inte rapporteras till tillsyns-myndigheten eller till de enskilda personerna eftersom det inte har varit tal om någon permanent förlust av tillgänglighet eller konfidentialitet. Om tillsynsmyndig-heten emellertid fick vetskap om incidenten på annat sätt kan den överväga att göra en undersökning för att bedöma efterlevnaden av de mer allmänna säkerhetskraven i artikel 32.

5. En person ringer en banks teletjänstcentral för att rapportera en personuppgiftsincident. Personen har fått någon annans månatliga kontoutdrag. Den personuppgifts ansvarige genomför en kort undersökning (som slutförs inom 24 timmar) och fastställer med rimlig säkerhet att en personuppgifts-incident har ägt rum och huruvida det finns en brist i systemet som innebär att andra personer har påverkats eller kan påverkas.	Ja.	Endast de personer som påverkades underrättas om det finns en hög risk och det är uppenbart att andra personer inte påverkades.	Om det efter en närmare undersökning visar sig att fler personer påverkas måste en uppdatering göras till tillsyns-myndigheten, och den personuppgifts-ansvarige ska vidta de ytterligare åtgärder som krävs genom att underrätta andra personer om det finns en hög risk för dem.
6. En personuppgifts-ansvarig driver en marknadsplats på nätet och har kunder i flera medlemsstater. Marknadsplatsen utsätts för ett it-angrepp och angriparen publicerar användarnamn, lösenord och köphistorik på nätet.	Ja, rapportera till ansvarig tillsynsmyndighet om det rör sig om gränsöverskridande behandling.	Ja, eftersom detta kan leda till en hög risk.	Den personuppgifts ansvarige bör vidta åtgärder, t.ex. att tvinga de berörda kontona att återställa lösenorden och andra åtgärder för att minska risken. Den personuppgifts ansvarige bör även överväga andra anmälningsskyldighe ter, t.ex. enligt NIS-direktivet som leverantör av digitala tjänster.

7. Ett webbhotell som fungerar som personuppgiftsbiträde noterar ett fel i den kod som styr användar-auktorisationen. Konsekvensen av bristen innebär att alla användare kan få tillgång till alla andra användares kontouppgifter.	Som personuppgifts biträde måste webbhotellet underrätta de berörda kunderna (de personuppgifts ansvariga) utan onödigt dröjsmål. Förutsatt att webbhotellet har gjort en egen undersökning bör de berörda personuppgiftsansvariga vara rimligen säkra på huruvida de har drabbats av en incident, och därför ska anses ha ”fått vetskap”, så snart de har underrättats av webbhotellet (personuppgiftsbiträdet). Den personuppgifts ansvarige ska därefter underrätta tillsynsmyndigheten.	Om det sannolikt inte finns någon hög risk för enskilda personer behöver dessa inte underrättas.	Webbhotellet (personuppgiftsbiträdet) måste överväga andra anmälningsskyldigheter (t.ex. enligt NIS-direktivet som leverantör av digitala tjänster). Om det inte finns något som tyder på att denna sårbarhet har utnyttjats av någon av de personuppgiftsansvariga är det inte säkert att incidenten behöver anmälas men den måste sannolikt registreras som ett exempel på bristande efterlevnad enligt artikel 32.
8. Patientjournaler på ett sjukhus är inte tillgängliga under 30 dagar på grund av ett it-angrepp.	Ja, sjukhuset är skyldigt att anmäla incidenten eftersom den kan leda till hög risk för patienternas välbefinnande och deras personliga integritet.	Ja, rapportera till de personer som påverkas.	
9. Personuppgifter från en stor mängd personer skickas av misstag till fel sändlista med över 1 000 mottagare.	Ja, rapportera till tillsynsmyndigheten.	Ja, rapportera till enskilda personer beroende på de berörda person-uppgifternas omfattning och typ och de potentiella konsekvens-ernas svårighetsgrad.	

10. Ett e-postmeddelande skickas till mottagare i fälten ”till:” eller ”cc:”, vilket gör det möjligt för alla mottagare att se andra mottagares e-postadress.	Ja, det kan vara obligatoriskt att anmäla incidenten till tillsyns-myndigheten om en stor mängd personer berörs, om känsliga uppgifter röjs (t.ex. en psykoterapeuts sändlista) eller om andra faktorer innebär en hög risk (t.ex. att e-postmeddelandet innehåller de ursprungliga lösenorden).	Ja, rapportera till enskilda personer beroende på de berörda person-uppgifternas omfattning och typ och de potentiella konsekvens-ernas svårighetsgrad.	En anmälan är eventuellt inte nödvändig om ingen känslig information röjs och endast ett litet antal e-postadresser har avslöjats.

Bilaga 2 Riskanalys

Genomför en riskanalys

Vid en riskanalys ska ni gå igenom nedanstående frågor. Om ni svarar ja på någon av följande punkter så kan det innebära att ni behöver genomföra en konsekvensbedömning. Om ni svarar ja på två (2) eller fler av punkterna så ska det i de allra flesta fall genomföras en konsekvensbedömning. I de fall ni är tveksamma till punkterna så bör det alltid genomföras en konsekvensbedömning.

Frågor	Ja	Nej
Utvärdering poängsättning		
1. Kommer personer utvärderas eller poängsättas?		
2. Förekommer profilering eller förutsägelser?		
3. Rör personuppgifterna arbetsprestation, ekonomisk situation, hälsa, personliga intressen, beteenden eller förflyttningar?		
Automatiserade beslut		
4. Innebär behandlingen ett automatiserat beslutsfattande som har rättsliga eller liknande följder för de registrerade? Ett system som fattar beslut utifrån uppgifter om en individ.		
5. Kan behandlingen leda till utestängning eller diskriminering?		
Systematisk övervakning		
6. Innebär behandlingen en systematisk övervakning av t.ex. ett nätverk?		
7. Innebär behandlingen att observera, övervaka eller kontrollera de registrerade? Exempelvis kameraövervakning på allmän plats.		
Känsliga personuppgifter eller av mycket personlig karaktär		
8. Sker behandling av känsliga personuppgifter (se avsnitt 7.1) eller uppgifter av mycket personlig karaktär (se avsnitt 7.3)?		
Uppgifter i stor omfattning		
9. Kommer personuppgifter att behandlas i stor omfattning?		
Matchande/kombinerade uppgiftsserier		
10. Kommer ni samköra olika register med varandra?		
Uppgifter som rör sårbara registrerade		
11. Rör behandlingen av personuppgifter sårbara personer (dvs. är det en maktobalans mellan den registrerade och den personuppgiftsansvarige? Exempelvis barn, anställda, psykiskt sjuka personer, asylsökande, äldre personer, patienter.		
Innovativ användning av nya tekniska/organisatoriska lösningar		
12. Kommer personuppgiftsbehandlingen användas i nya tekniska eller organisatoriska lösningar eller brukas på ett nytt och innovativt sätt?		
Begränsningar i utövandet av rättighet eller tjänst		
13. Hindrar behandlingen de registrerade från att utöva en rättighet eller använda en tjänst eller ett avtal?		

Bilaga 3 Konsekvensbedömning - Exempel

Beskriv behandlingen:	
Syftet med behandlingen:	
Laglig grund:	
Vilka risker för de registrerade har identifierats?	
Vilka åtgärder kommer genomföras för att minska riskerna – ange vilka risker respektive åtgärd minskar samt i vilken omfattning:	
Är behandlingen proportionerlig	Beskriv er bedömning gällande om behandlingen står i proportion till syftet med behandlingen.
Synpunkter från dataskyddsombudet:	Ange datum samt vad dataskyddsombudet haft för synpunkter.
Synpunkter från de registrerade:	Ange datum samt vad synpunkterna var.

Moment	**Har momentet uppfyllts?**	**Risker om momentet inte uppfyllts**	**Hanteras risken vidare?**	**Typer av konsekvenser**	**Allvarlig-hetsgrad (5 högst)**	**Förslag på åtgärder (skriv vilka ni väljer)**	**Allvarlig-hetsgrad efter genomförda åtgärder (5 högst)**
Registerförteckning							
Finns behandlingen med i registerförteckningen och uppfyller uppgifterna i registret samtliga krav enligt artikel 30 GDPR?	☐ Ja ☐ Nej	Registerförteckning saknas eller är inte komplett: behandlingen har inte kartlagts.	☐ Ja ☐ Nej	Förutsättningar för behandlingen är inte etablerade och beskrivna.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Genomför en dokumentation av behandlingen och fyll i samtliga uppgifter som krävs enligt artikel 30 GDPR.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Uppgifternas känslighetsgrad							
Har uppgifterna i behandlingen känslighets-/informationssäkerhetsklassats?	☐ Ja ☐ Nej	Brister i känslighets-/informationssäkerhets klassning	☐ Ja ☐ Nej	Känsliga uppgifter sprids till obehöriga med brott mot integritetsskyddet som följd.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Genomför klassning. **Om ja**: ange nivån som klassningen resulterade i.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Åtkomststyrning och kontroll							
Skydd av inloggning: finns täckande kontroll av identitet (autentisering) vid inloggning till behandlingen?	☐ Ja ☐ Nej	Brister i inloggning, förstärkt inloggning med tvåfaktor saknas till behandlingen	☐ Ja ☐ Nej	Uppgifter läcker till obehöriga, med brott mot integritetsskyddet som följd.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Bevaka och inför tvåfaktorsinloggning till behandlingen för åtkomstkontroll.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Behörighetshantering: finns rutiner för kontroll/uppföljning av att registrerade behörigheter är aktuella för samtliga användare?	☐ Ja ☐ Nej	Brister i behörighetshantering.	☐ Ja ☐ Nej	Uppgifter läcker till obehöriga, med brott mot integritetsskyddet som följd.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Administrera behörigheterna inom kommunen så att personal får legitim behörighet,	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Åtkomstloggning: Går det att upptäcka vem som har haft åtkomst till uppgifterna?	☐ Ja ☐ Nej	Brister i åtkomstloggning.	☐ Ja ☐ Nej	Det går inte att fastställa vem som haft åtkomst till extra skyddsvärda uppgifter.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Tillämpa loggning och loggkontroller.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Uppgiftsminimering (uppgifterna matchar ändamålen med behandlingen)							
Används uppgifter i behandlingen för **andra ändamål än de som framgår av** registerförteckningen?	☐ Ja ☐ Nej	Brister i ändamåls-styrning.	☐ Ja ☐ Nej	Uppgifter används för andra ändamål än de angivna vilket saknar laglig grund.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Avgränsa behandlingen så att uppgifter endast används för de angivna (godkända) ändamålen. Minimera mängden uppgifter i behandlingen.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Kan de registrerades **personnummer** ses av användare som inte behöver åtkomst till denna personuppgift?	☐ Ja ☐ Nej	Brister i dataskydd. Uppgiftsminimering uppnås inte.	☐ Ja ☐ Nej	Personnummer är tillgängliga för obehöriga vilket medför viss integritetsrisk.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Inför behörighets-begränsning för åtkomst till personnummer. Via behörighetsroller för ökad uppgiftsminering. Inför pseudonymisering eller avidentifiering av personuppgifter.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Om extra skyddsvärda uppgifter behandlas: har **pseudonymisering** införts för att begränsa åtkomsten till personuppgifter för de användare som inte behöver ha direkt åtkomst till dessa uppgifter?	☐ Ja ☐ Nej	Brister i dataskydd. Uppgiftsminimering uppnås inte.	☐ Ja ☐ Nej	Extra skyddsvärda uppgifter sprids till obehöriga.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Inför pseudonymisering eller avidentifiering av personuppgifter.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Har **behörigheter minimerats** för att undvika att fler personuppgifter för registrerade kan ses av användare utöver vad som krävs för dessa användares arbetsuppgifter?	☐ Ja ☐ Nej	Brister i behörighetshantering.	☐ Ja ☐ Nej	Personuppgifter sprids till obehöriga.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Inför behörighetsroller som är anpassade till verkliga åtkomstbehov för användarna. Säkerställ att samtliga användare har tilldelats rätt behörighetsroll(er).	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Förekommer **fritextfält** i registreringen?	☐ Ja ☐ Nej	Brister i dataskydd. Uppgiftsminimering uppnås inte.	☐ Ja ☐ Nej	Kan medföra att skyddsvärda uppgifter sprids till obehöriga eller att vi samlar in fler uppgifter än vad vi behöver för ändamålet.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Säkerställ att förekomst av fritextfält minimeras i behandlingen. Säkerställ att åtkomst till fritextfält behörighets begränsas till endast de användare som behöver denna åtkomst. Skriv en förklarande text bredvid fritextfältet så att den registrerade förstår vad som denne bör skriva respektive inte skriva.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
<u>Om ja</u> på föregående punkt, har **användningen av fritextfält** reglerats i rutin (vad som får skrivas i fritextfält) utifrån perspektivet med minimering av extra skyddsvärda personuppgifter?	☐ Ja ☐ Nej	Brister i dataskydd. Uppgiftsminimering uppnås inte.	☐ Ja ☐ Nej	Kan medföra att skyddsvärda uppgifter sprids till obehöriga eller att vi samlar in fler uppgifter än vad vi behöver för ändamålet.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Säkerställ att rutin finns för vad som får skrivas i fritextfält för att undvika att extra skyddsvärda uppgifter sprids till obehöriga via dessa fält.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Lagringsminimering & gallring							
Har det identifierats en nödvändig **lagringstid** för uppgifterna i behandlingen i relation till de behov som finns med ändamålen?	☐ Ja ☐ Nej	Lagringsminimering uppnås inte.	☐ Ja ☐ Nej	Lagringsminimering uppnås inte, spridning av extra skyddsvärda uppgifter som inte behöver vara åtkomliga.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Definiera nödvändig lagringstid för uppgifterna baserat på angivna ändamål med behandlingen. Uppdatera dokumenthanteringsplaner/gallringsrutiner. Ta fram schema för radering av uppgifterna efter den nödvändiga lagringstiden.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Har mer uppgifter lagrats än vad som är nödvändigt för behandlingen?	☐ Ja ☐ Nej	Lagringsminimering uppnås inte.	☐ Ja ☐ Nej	Lagringsminimering uppnås inte, spridning av extra skyddsvärda uppgifter som inte behöver vara åtkomliga.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Minimera mängden uppgifter i behandlingen. Begränsa informationen som används för specifika syften, med stark juridisk, organisatorisk och teknisk säkerhet för att förhindra att uppgifterna används för andra syften.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Finns behandlingen med i **dokumenthanterings-plan / gallringsrutin**?	☐ Ja ☐ Nej	Lagringsminimering uppnås inte.	☐ Ja ☐ Nej	Se konsekvenserna i momenten ovan.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Uppdatera dokumenthanterings-plan samt eventuella gallringsrutiner.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Finns möjlighet till **arkivering** av uppgifter som inte längre är aktuella (om krav på lagring av uppgifterna finns så att de inte får gallras)?	☐ Ja ☐ Nej	Brister i dataskydd. Uppgifts- och lagrings-minimering uppnås inte.	☐ Ja ☐ Nej	Lagringsminimering uppnås inte, spridning av extra skyddsvärda uppgifter som inte behöver vara åtkomliga för den dagliga verksamheten.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Ta fram en arkiveringsrutin och inför arkiverings-funktioner för behandlingen.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Om ja på föregående punkt: Har **åtkomsten till arkiverade uppgifter begränsats** till ett fåtal behöriga användare?	☐ Ja ☐ Nej	Brister i dataskydd. Uppgiftsminimering uppnås inte.	☐ Ja ☐ Nej	Lagringsminimering uppnås inte, spridning av extra skyddsvärda uppgifter som inte behöver vara åtkomliga för den dagliga verksamheten.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Begränsa åtkomsten till arkiverade uppgifter till ett fåtal användare som behöver denna behörighet.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Utlämning av uppgifter till extern part							
Lämnas uppgifter ut **till extern part** utan att ett gällande biträdesavtal finns?	☐ Ja ☐ Nej	Brister i dataskydd. Brister i biträdeshantering – biträdesavtal saknas.	☐ Ja ☐ Nej	Extra skyddsvärda uppgifter sprids till obehöriga med brott mot integritetsskyddet som följd.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Säkerställ att uppgifter i behandlingen endast lämnas ut till externa parter efter att en prövning gjorts för utlämningen. Säkerställ att biträdesavtal eller att ett motsvarande standardavtal finns som täcker kraven för dataskydd i biträdeshantering.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Sker överföring av uppgifter i behandlingen till **tredje land**?	☐ Ja ☐ Nej	Brister i tredjeland-överföring i form av att säkerhetskraven inte är uppfyllda.	☐ Ja ☐ Nej	Uppgifter lagras i tredjeland utan överenskommelse/lagrum för tillräckligt dataskydd uppgifter till land/länder utanför EU/EES.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Säkerställ att uppgifter i behandlingen inte kan nås från/lämnas ut till tredjeland. Säkerställ att adekvat skyddsnivå finns.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Kan vi upptäcka om personuppgifter läcker ut till obehöriga?	☐ Ja ☐ Nej	Brister i rutin eller säkerhet kring behandling av personuppgifter.	☐ Ja ☐ Nej	Incidentrapportering kan inte ske (inom GDPR:s krav på tidsperiod) till tillsynsmyndighet. Vi kan inte informera de registrerade om läckan.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Säkerställ att läckage av uppgifter kan upptäckas då det sker så att incident-rapportering kan ske inom GDPR:s krav (72 timmar från upptäckt) samt att vi kan informera de registrerade i de fall det finns behov.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Den registrerades rättigheter							
Har nödvändig och tillräcklig **information givits till den registrerade** om behandlingen?	☐ Ja ☐ Nej	Brister i informations-givning. Brister i transparens.	☐ Ja ☐ Nej	Tillräcklig information om behandlingen kan inte ges till den registrerade.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Säkerställ att tillräcklig information kan lämnas till den registrerade om vad som registreras och för vilka ändamål mm. Säkerställ att informationen görs mer transparent för att informera den registrerade.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Om samtycke används som laglig grund för behandlingen: Har rutin för **samtyckes-hantering** etablerats för behandlingen?	☐ Ja ☐ Nej	Brister i samtyckeshantering.	☐ Ja ☐ Nej	Att inhämtning och dokumentering av samtycken inte uppfyller kraven i GDPR.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Ta fram en rutin som säkerställer att samtycke kan inhämtas och dokumenteras för behandlingen.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Finns möjlighet att ta ut uppgifter till ett **registerutdrag** på begäran av den registrerade?	☐ Ja ☐ Nej	Brister i register-utdragshantering.	☐ Ja ☐ Nej	Registerutdrag kan inte skapas och levereras för behandlingen till den registrerade.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Ta fram en rutin för att säkerställa att registerutdrag kan skapas och tillhandahållas till den registrerade.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Finns rutin för hur **rättelse** av personuppgifter ska ske på begäran av den registrerade?	☐ Ja ☐ Nej	Brister i rättningshanteringen.	☐ Ja ☐ Nej	Uppgifter riskerar att vara felaktiga (inaktuella, ej korrekta). Vi kan inte tillgodose den registrerades rätt till rättelse.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Ta fram en rutin för att säkerställa att rättelse eller radering sker när så ska ske.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Om det är aktuellt med rättelse finns möjlighet till det i t.ex. IT-systemet?	☐ Ja ☐ Nej	Brister i rättningshanteringen.	☐ Ja ☐ Nej	Uppgifter riskerar att vara felaktiga (inaktuella, ej korrekta). Vi kan inte tillgodose den registrerades rätt till rättelse.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Vid upphandling av t.ex. IT-system så ska det säkerställas att det finns funktioner för rättelse som uppfyller kraven i GDPR.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Radering (rätten att bli glömd, om samtycke används som rättslig grund för behandlingen): Finns det en rutin för hur radering av personuppgift ska ske på begäran av den registrerade?	☐ Ja ☐ Nej	Brister i raderingshantering.	☐ Ja ☐ Nej	Uppgifter riskerar att inte kunna raderas på begäran av den registrerade i de fall vi faktiskt ska radera uppgifterna enligt GDPR (”rätten att bli glömd” kan inte tillgodoses för den registrerade).	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Ta fram en rutin för att säkerställa att radering av uppgifter i behandlingen kan göras på begäran av den registrerade i de fall vi ska radera uppgifterna enligt GDPR.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5a
Om det är aktuellt med **radering** finns möjlighet till det i t.ex. IT-systemet?	☐ Ja ☐ Nej	Brister i raderingshantering.	☐ Ja ☐ Nej	Uppgifter riskerar att inte kunna raderas på begäran av den registrerade i de fall vi faktiskt ska radera uppgifterna enligt GDPR (”rätten att bli glömd” kan inte tillgodoses för den registrerade).	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Vid upphandling av t.ex. IT-system så ska det säkerställas att det finns funktioner för radering som uppfyller kraven i GDPR.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Finns rutin för hur **begränsning av behandling** ska ske på begäran av den registrerade?	☐ Ja ☐ Nej	Brister i hanteringen av rätten till begränsning av behandling.	☐ Ja ☐ Nej	Uppgifter riskerar att inte kunna markeras (begränsas) så att de endast får behandlas för vissa avgränsade syften.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Ta fram en rutin för att säkerställa att begränsning av behandling kan ske på begäran av den registrerade när så ska ske.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Om det är aktuellt med begränsning av behandling finns möjlighet till det i t.ex. IT-systemet?	☐ Ja ☐ Nej	Brister i hanteringen av rätten till begränsning av behandling.	☐ Ja ☐ Nej	Uppgifter riskerar att inte kunna markeras (begränsas) så att de endast får behandlas för vissa avgränsade syften.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Vid upphandling av t.ex. IT-system så ska det säkerställas att det finns funktioner för begränsning av behandling som uppfyller kraven i GDPR.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Inbyggt dataskydd (”Privacy by design”)							
Har kraven på **inbyggt dataskydd** gåtts igenom för behandlingen?	☐ Ja ☐ Nej	Brister i dataskydd.	☐ Ja ☐ Nej	Otillräckligt skydd av uppgifter, spridning av extra skyddsvärda uppgifter till obehöriga eller förlust av uppgifter.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Om ny IT-tjänst/systemstöd ska anskaffas ska en kravlista användas som underlag.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Kan det förhindras eller upptäckas om **uppgifter förändrats felaktigt** (oavsiktligt eller avsiktligt)?	☐ Ja ☐ Nej	Brister i riktighetskontroll.	☐ Ja ☐ Nej	Uppgifter förvanskas och blir felaktiga/korrupta.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Säkerställ att användare inte kan förändra uppgifter utan att de upptäckts (indatakontroller/granskningar samt loggkontroller/spårbarhet).	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Bedöms behov finnas av **kryptering** av information i behandlingen för att minimera riskerna för obehörig åtkomst?	☐ Ja ☐ Nej	Brister i dataskydd (integritet).	☐ Ja ☐ Nej	Otillräckligt skydd av uppgifter, spridning av extra skyddsvärda uppgifter till obehöriga.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Överväg om kryptering ska införas för överföring och/eller lagring av uppgifter i behandlingen.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Om ja på föregående fråga, **har kryptering införts** (för dataöverföring, databas/ lagring)?	Över-föring: ☐ Ja ☐ Nej Lagring: ☐ Ja ☐ Nej	Brister i dataskydd (integritet)	☐ Ja ☐ Nej	Otillräckligt skydd av uppgifter, spridning av extra skyddsvärda uppgifter till obehöriga.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Säkerställ att kryptering har införts för överföring och/eller lagring av uppgifter i behandlingen enligt beslut i föregående åtgärd.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Finns möjlighet att skydda uppgifter från att oavsiktligt förstöras/raderas (via backup/motsvarande)?	☐ Ja ☐ Nej	Brister i tillgänglig-hetsskydd.	☐ Ja ☐ Nej	Uppgifter förstörs oavsiktligt, uppgifter ska skyddas från oavsiktlig radering/förstöring.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Säkerställ att uppgifter kan skyddas från oavsiktlig radering/förstöring (via adekvat backup).	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Avtal och personuppgiftsbiträden							
Finns aktuellt **biträdesavtal** (enligt kraven i GDPR) upprättat med samtliga personuppgiftsbiträden, om sådana biträden finns?	☐ Ja ☐ Nej	Brister i biträdeshantering.	☐ Ja ☐ Nej	Vi har otillräckligt avtalsskydd för vår behandling och riskerar att kraven i GDPR och svensk rätt inte efterlevs.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Upprätta biträdesavtal med samtliga personuppgiftsbiträden	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Om ja på föregående punkt: uppfyller biträdesavtalen kraven i GDPR?	☐ Ja ☐ Nej	Brister i biträdeshantering / otillräckligt avtalsskydd.	☐ Ja ☐ Nej	Vi har otillräckligt avtalsskydd för vår behandling och riskerar att kraven i GDPR och svensk rätt inte efterlevs.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Säkerställ att samtliga biträdesavtal uppfyller kraven i GDPR.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5
Rådfrågan av kommunens dataskyddsombud							
Har dataskyddsombudet rådfrågats gällande behandlingen av personuppgifter?	☐ Ja ☐ Nej	Samordning och avstämning av kravuppfyllnad för behandlingen har inte gjorts.	☐ Ja ☐ Nej	Det är oklart om kraven i GDPR och svensk rätt efterlevs samt om tillräckliga skyddsåtgärder har planerats.	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5	Rådfråga dataskyddsombudet. Kravet gäller endast vid behandling av känsliga/extra skyddsvärda personuppgifter (för vilka behandlingar en konsekvensbedömning såsom denna ska upprättas)	☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Personuppgiftsstrategi

För Samhällsbyggnadsförbundet Bergslagen

Antagen av direktionen 2021-XX-XX

1. Inledning

Sedan den 25 maj 2018 gäller EU:s dataskyddsförordning[1] (nedan dataskyddsförordningen). Denna strategi beskriver förbundets hantering av personuppgifter på övergripande nivå för att säkerställa att kraven i dataskyddsförordningen samt övrig gällande rätt på området följs. Strategin gäller vid all behandling av personuppgifter inom förbundet och kompletterar övriga styrdokument.

Strategin gäller för förbundet, direktion, avdelningar, medarbetare och förtroendevalda politiker. Eftersom alla verksamheter omfattas av strategin finns inte utrymme för att besluta om lokala regler som avviker från denna.

2. Behandling av personuppgifter

En personuppgift (enligt dataskyddsförordningen) är varje upplysning som avser en identifierad eller identifierbar levande fysisk person (nedan registrerade) såsom exempelvis namn, personnummer och adress. Definitionen av begreppet behandling av personuppgifter är vid och omfattar i princip alla åtgärder som sker i fråga om personuppgifter. Några exempel är insamling, registrering, lagring, läsning och radering.

3. Målsättning

Strategin fastställer övergripande mål och intentioner för behandling av personuppgifter. All behandling av personuppgifter ska ske med hänsyn till den registrerades friheter och rättigheter varför vi ska vara öppna med hur vi samlar in, bearbetar och delar med oss av de personuppgifter vi behandlar. Innebörden i detta är att värna om den personliga integriteten så att alla registrerade är trygga i att förbundet eftersträvar en hög nivå av skydd för personuppgifter.

Målen vid all personuppgiftsbehandling ska vara att

- ✓ Behandling ska ske i enlighet med gällande rätt samt ske på ett korrekt och öppet sätt i förhållande till den registrerade. Detta inkluderar att informera de registrerade om våra behandlingar av personuppgifter samt vilka rättigheter de har.
- ✓ Behandling ska endast ske om det finns ett fastställt berättigat ändamål (ändamålsbegränsning).
- ✓ Uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).
- ✓ Uppgifterna ska vara riktiga och om nödvändigt uppdaterade.
- ✓ Uppgifterna ska bevaras i identifierbar form så länge det är nödvändigt för ändamålet (lagringsminimering).
- ✓ Risker för skada för den registrerade ska minimeras genom aktiv riskhantering och lämpliga tekniska och organisatoriska säkerhetsåtgärder.
- ✓ Endast behöriga ska få åtkomst till personuppgifter.

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

- ✓ Personuppgifter ska skyddas så de inte förstörs oavsiktligt.
- ✓ Verksamheten ska tillämpa inbyggt dataskydd genom att uppdatera, rensa och underhålla befintliga systemstöd och rutiner samt ta hänsyn till detta vid kravställning vid inköp, design eller utveckling.
- ✓ Verksamheten ska tillämpa principen om dataskydd som standard, d.v.s. bygga in uppgiftsminimering i systemen och inte ta in eller registrera mer uppgifter än de som verkligen är nödvändiga.
- ✓ Ha en god förmåga att hantera personuppgiftsincidenter och om kriterierna är uppfyllda anmäla incidenten till tillsynsmyndigheten.
- ✓ Alla medarbetare och förtroendevalda fortlöpande får information och utbildning inom området.
- ✓ Överföring till tredje land (utanför EU/EES) inte sker utan adekvata säkerhetsåtgärder.
- ✓ Behandlingen ska finnas dokumenterad i ett register över behandling en s.k. registerförteckning.
- ✓ I de fall den utförs av ett personuppgiftsbiträde även åtföljs av ett giltigt personuppgiftsbiträdesavtal eller en annan rättsakt.
- ✓ Behandlingen riskbedöms och i de fall den innebär en hög risk för de registrerades fri- och rättigheter ska en konsekvensbedömning genomföras.

4. Roller och ansvar

Direktionen beslutar övergripande om viljeinriktning för personuppgiftsarbetet utöver denna strategi.

Personuppgiftsansvarig är direktionen. Personuppgiftsansvarig är den bestämmer ändamålen och medlen med en behandling av personuppgifter, det vill säga varför och hur behandlingen ska gå till. Personuppgiftsansvarig är ansvarig för att all hantering av personuppgiftering som sker i deras verksamhet. Det innebär att det är personuppgiftsansvarig som är ansvarig för att målen och intentionerna i denna strategi efterlevs i den verksamhet som de ansvarar för.

Förutom att uppfylla målen ska varje personuppgiftsansvarig

- ✓ Utse ett dataskyddsombud samt tillse att dennes kontaktuppgifter blir offentliggjorda samt anmälda till tillsynsmyndigheten.
- ✓ Utse flera personuppgiftssamordnare inom förvaltningen.

Ett **dataskyddsombud** ska vara utsett av varje personuppgiftsansvarig för att bland annat ge information samt granska hur verksamheten lever upp till kraven i dataskyddsförordningen.

Personuppgiftssamordnare ska vara förbundets huvudsakliga kontaktperson vid frågor rörande personuppgifter och dataskydd, varför rollen som personuppgiftssamordnare förutsätter en organisatorisk position som sitter nära förvaltningens ledning. Samordnaren ska även agera som förmedlande länk mellan förbundet och dataskyddsombudet. Uppdraget som personuppgiftssamordnare är primärt inom förbundet, men arbetsuppgifter kan även förekomma inom andra förvaltningar i kommunen om behov finns p.g.a. semester eller liknande.

Dataskyddsgruppen är ett nätverk för personuppgifts- och dataskyddsfrågor. Nätverket är till för att stötta verksamheten samt personuppgiftssamordnarna i sitt arbete samt är verksamhetens främsta kontaktyta mellan personuppgiftssamordnare och dataskyddsombud.

Medarbetare har ett ansvar för att följa förbundets beslutade styrdokument i form av t.ex. strategier och riktlinjer. Varje medarbetare ansvarar även för att följa dokumenthanteringsplaner, gallringsrutiner och vara uppmärksam på brister och personuppgiftsincidenter och anmäla dessa vidare internt.