Dataskyddsombudets granskningsrapport - Hylte kommun 2019

Diarienummer	KS 2019/81
Ansvarig	Jessica Karlsson, Dataskyddsombud för Hylte, Laholm och Falkenbergs kommuner
Granskning av följande Personuppgiftsansvariga nämnder och styrelser	Arbets- och näringslivsnämnden, Omsorgsnämnden, Kommunstyrelsen, Samhällsbyggnadsnämnden, Barn- och ungdomsnämnden, Valnämnden, Bostadsstiftelsen Hyltebostäder, Tillsynsnämnden

Falkenbergs kommun, 31180 Falkenberg
Telefon växel: 0346-88 60 00
e-post: kontaktcenter@falkenberg.se
kommun.falkenberg.se

Innehåll

1. Sammanfattning....4

2. Bakgrund, metod och syfte....7
2.1 Bakgrund och metod....7
2.2 Syfte....7

3. Redovisning av svar....8

3.1 Har er nämnd/styrelse utsett personuppgiftssamordnare och registerförtecknare....8

3.2 Har kommunen en utpekad, centralt placerad samordnare för kommunens totala informationssäkerhetsarbete?....9

3.3 Har era personuppgiftssamordnare/motsvarande genomgått någon extern utbildning i GDPR....9

3.4 Har ni gjort er kartläggning av personuppgiftsbehandlingar och upprättat registerförteckningar?....10

3.5 Har ni identifierat era personuppgiftsbiträden och tecknat biträdesavtal?....11

3.6 Har ni en fastställd rutin/process för uppdatering och uppstart av nya personuppgiftsbehandlingar?....13

3.7 Har ni en fastställd process för begäran om registerutdrag?....13

3.8 Har ni en fastställd rutin för incidenthantering?....14

3.9 Behandlar ni särskilda kategorier personuppgifter?....14

3.10 Har ni gjort en konsekvensbedömning för behandlingen?....15

3.11 Har ni en lösning på plats för att digitalt kunna kommunicera känsliga personuppgifter och sekretessbelagd information?....15

3.12 Har ni en lösning för att säkerställa säkra utskrifter av dokument?....16

3.13 Har ni en plan för hur ni ska kunna upprätthålla ett långsiktigt arbete kring personuppgiftsbehandling och dataskydd?....16

3.14 Finns det en i er kommun samordnad och tydlig process för hur upphandling av IT-system/tjänster ska gå till?....17

3.15 Om en process finns, är det i den även uttryckt vilka roller som deltar och vilka deras uppgifter är?....17

4. Analys, diskussion och slutsats....26

4.1 Rollen PUS är utsedd i de flesta nämnder och styrelser....26

4.2 Kommunen har en samordnare för kommunens totala informationssäkerhetsarbete....27

4.3 De flesta av personuppgiftssamordnarna har genomgått en intern utbildning i GDPR....29

4.4 Verksamheterna har kommit olika långt i sitt arbete med registerförteckningar....30

4.5 Det återstår en hel del arbete med att identifiera biträden och teckna avtal.30

4.6 Det saknas rutin för hur fånga upp förändrade/nya personuppgiftsbehandlingar....32

4.7 Process för registerutdrag saknas....33

4.8 Process för incidenthantering saknas....33

4.9 Behandling av särskilda kategorier personuppgifter sker i olika grad inom alla nämnder och styrelser....34

4.10 Nämnder och styrelser arbetar inte alls med risk- och konsekvensbedömningar....34

4.11 Verktyg för säker digital kommunikation finns delvis på plats....35

4.12 Lösning för säkra utskrifter är på plats....36

4.13 Det saknas planer för ett långsiktigt arbete med personuppgifter och dataskydd……37

4.14 En samordnad process för hur behov av nya IT-lösningar ska hanteras är inte implementerad……38

Bilaga 1. Definitioner och förklaringar av begrepp……41

1. Sammanfattning

En av dataskyddsombudets arbetsuppgifter är att granska den personuppgiftsansvariges efterlevnad av GDPR (General Data Protection Regulation/Dataskyddsförordningen). Personuppgiftsansvarig, d v s ytterst ansvarig för den personuppgiftsbehandling som sker, är inom kommunal verksamhet respektive nämnd eller styrelse.

Under första halvåret 2019 fick samtliga nämnder och styrelser i Hylte ett frågeunderlag att besvara. Svaren utgör underlag för granskningen och denna rapport. Denna första granskning rör i stort sett förutsättningarna för verksamheterna att överhuvudtaget kunna arbeta med och försöka leva upp till de krav som lagstiftningen, GDPR, ställer på alla de som hanterar personuppgifter. Syftet med granskningen har också varit att få en nulägesbild av var verksamheterna befinner sig i arbetet och att granskningsrapporten ska utgöra stöd och hjälp i det fortsatta arbetet.

I granskningen framkommer att verksamheterna har gjort ett stort arbete med anpassningen till GDPR. Men, precis som i de flesta kommuner, så var arbetet utifrån den tidigare gällande personuppgiftslagen eftersatt och det trots att den innehöll liknande hårda krav som den nya lagstiftningen GDPR. Det som fick fart på hela Europas arbete med personuppgiftshanteringen var nog att det med GDPR infördes sanktionsavgifter för de som inte uppfyller lagens krav. Den kraftiga digitaliseringen har säkert också bidragit till att integritetsfrågorna kommit i fokus.

Mycket arbete återstår dock i kommunen, samtidigt som det är ett arbete som aldrig blir eller kan bli färdigt, det måste bedrivas systematiskt och kontinuerligt.

Det som bör prioriteras av de personuppgiftsansvariga och ledningen i Hylte kommun är att;

- verka för att det snarast skapas en kommungemensam process med rutiner över hur en begäran om registerutdrag ska hanteras
- verka för att det snarast skapas en kommungemensam process med rutiner för incidenthantering och att den sedan tidigare klara e-tjänsten tas i bruk
- verka för att ett forum/nätverk för PUS och RF snarast startas upp – regelbundna möten för information/utbildning, erfarenhetsutbyte och samarbete inom områdena GDPR och informationssäkerhet
- säkerställa att rollen personuppgiftssamordnare, PUS, för respektive nämnd/styrelse finns på plats, t ex inom Tillsynsnämnden och Samhällsbyggnadsnämnden som angett att man inte har sådan på plats
- överväga att utse registerförtecknare, RF, och speciellt inom de nämnder som är stora och breda i sin verksamhet.
- verka för att organisationen blir väl insatt i vad rollerna PUS och RF innebär, uppgifter och omfattning
- verka för att det snarast upprättas en kommungemensam plan med prioriterade arbetsområden avseende arbetet med GDPR
- prioritera anordnandet av utbildningar inom informationshantering - GDPR, TF, OSL m.fl.

- verka för att skapa en metod för hur kartläggning av personuppgiftsbehandlingar i ostrukturerat material ska göras
- verka för att arbetet med identifierandet av biträden och tecknandet av biträdesavtal fullföljs
- klargöra vem som ska teckna biträdesavtal och fastslå det i lämpliga styrdokument
- säkerställa att biträdesavtal tecknas samtidigt som huvudavtal tecknas
- verka för att Hylte kommuns utkast till ”Process för införande av nya system” färdigställs samt kompletteras så att den får ett ökat fokus på verksamheternas behov och att ett kommunövergripande samarbete genomsyrar modellen samt att den därefter beslutas
- säkerställa ifall behandling sker av särskilda kategorier personuppgifter och även av i övrigt integritetskänsliga personuppgifter
- verka för att verksamheterna arbetar med konsekvensbedömningar
- verka för att en användarautentiseringslösning (IdP) snarast kommer på plats och att lösningen Trusted Dialog därefter tas i bruk
- verka för att alla verksamheter nyttjar Follow Me Print
- säkerställa att arbetet med dataskydd enligt GDPR och det totala arbetet med informationssäkerhet arbetas in i kommunens redan etablerade processer för planering ledning, styrning och kontroll
- verka för att en specifik person tilldelas ansvaret för de tekniska informationssäkerhetsfrågorna i kommunen

Ovanstående uppräkning utgör inte samtliga råd och rekommendationer, se vidare under respektive analysavsnitt i rapporten.

Om inte en verksamhet ges de rätta förutsättningarna att arbeta med personuppgifts- och informationssäkerhetsfrågor, då kan kommunen aldrig leva upp till lagstiftningens krav och det finns stor risk för att de registrerades integritet inte skyddas samt att kommunen drabbas av sanktionsavgifter. Om kommunen inte kan upprätthålla lämplig säkerhetsnivå för sin information inklusive personuppgifter, då riskerar även kommunen att tappa förtroendekapital hos medborgarna. Ordning och reda på kommunens information samt kunskap om den och dess värde, det utgör grunden för att kunna digitalisera arbetsprocesser och skapa digitala tjänster till nytta för dem som kommunen är till för, kommuninvånarna.

2. Bakgrund, metod och syfte

2.1. Bakgrund och metod

Dataskyddsombudets arbetsuppgifter och ställning framgår av Artikel 38–39 GDPR (General Data Protection Regulation) med förtydliganden i Artikel 29-gruppens riktlinjer om dataskydd.
En av dataskyddsombudets arbetsuppgifter är att övervaka efterlevnaden av GDPR och andra av unionens eller medlemsstaternas dataskyddsbestämmelser samt av den personuppgiftsansvariges riktlinjer för skydd av personuppgifter. Personuppgiftsansvarig, d v s ytterst ansvarig för den personuppgiftsbehandling som sker inom dess verksamhet, är respektive nämnd eller styrelse.

Som ett led i skyldigheten att övervaka efterlevnaden kan dataskyddsombudet;

- samla in information för att identifiera hur behandling av personuppgifter sker
- analysera och kontrollera huruvida bestämmelser om behandlingen efterlevs och
- informera samt ge råd och utfärda rekommendationer till den person uppgiftsansvarige.

Under första halvåret 2019 samlades underlag för granskning in från samtliga nämnder och styrelser. Granskningen rör i stort sett förutsättningarna som verksamheterna har för att kunna arbeta systematiskt med området personuppgiftsbehandling enligt bl. a GDPR. Dataskyddsombudet önskade svar på 16 stycken frågor. Inkomna svar har sammanställts och analyserats i denna granskningsrapport. Dataskyddsombudet pekar även på ett antal åtgärder som bör vidtas med anledning av vad som framkommit i granskningen. Rapporten delges nämnder och styrelser samt kommunchef och förvaltningsledningar. Vid behov kommer dataskyddsombudet att göra uppföljningar av granskningen. Resultaten för Hylte kommuns nämnder och styrelser presenteras här i en och samma rapport.

Se bilaga 1 för definition och förklaringar av diverse begrepp från dataskyddsförordningen mm.

2.2. Syfte

Syftet med dataskyddsombudets granskning i detta fall var att få en bild av nämnder och styrelsers förutsättningar till regelefterlevnad av GDPR och det bl.a. ur ett organisatoriskt perspektiv - finns roller utpekade med särskilt ansvar för arbetet, hur ser kompetensen ut hos de med särskilt ansvar vad gäller personuppgiftshantering, finns lösning för säker digital kommunikation etc.?

Granskningen har också fokus på ett par processer som direkt eller indirekt påverkar person-uppgiftshanteringen och säkerheten för dessa. Resultatet av granskningen ska ses som en hjälp för de personuppgiftsansvariga i sitt fortsatta arbete med personuppgiftshantering och vilka områden som bör prioriteras.

3. Redovisning av svaren, fråga för fråga

Svaren från nämnderna och styrelserna redovisas i princip fråga för fråga nedan. I några fall har ett par frågor och svar slagits ihop i ett och samma avsnitt då de är nära förknippade med varandra.

3.1. Har er nämnd/styrelse utsett personuppgiftssamordnare (PUS) samt registerförtecknare (RF)?

Enligt ett kommunövergripande beslut gäller att personuppgiftssamordnarna ansvarar för och samordnar personuppgiftsbehandlingarna i det operativa arbetet. De som utses som personuppgifts-samordnare ska vara kontaktperson till dataskyddsombudet. Personerna ska inneha sakkunskap om gällande regler och vara ett stöd till verksamheten i frågorna. De ska se till att kompetensutveckling garanteras i den egna verksamheten. Som personuppgiftssamordnare ska man särskilt jobba för att verksamheten fångar upp och registrerar nya behandlingar av personuppgifter. Personuppgifts-samordnarna utför sitt uppdrag inom ramen av sin ordinarie tjänst. Utbildningar och andra kostnader ska täckas inom ramen för respektive tjänst.
Registerförtecknare har kommunen inte utsett. Många av de utsedda personuppgiftssamordnarna har även verkat som registerförtecknare. Om man behöver utse registerförtecknare är upp till verksamheterna att avgöra men det kan vara lämpligt om verksamheten är stor eller har ett brett uppdrag.

Arbets- och näringslivsnämnden, ANN, i Hylte kommun har utsett en personuppgiftsamordnare för var och en av sina verksamheter Fritid- och folkhälsa, Individ- och familjeomsorg vuxen och Bibliotek och kultur. Dessutom har frågan lyfts på arbetsmarknadsenheten om de behöver utse en egen personuppgiftssamordnare eller om det räcker att de har en registrator.

Omsorgsnämnden, ON, i Hylte kommun har 2018-09-13 beslutat att utse system-administratör/avgiftshandläggare som personuppgiftssamordnare.

Barn- och ungdomsnämnden, BUN, i Hylte kommun har 2018-09-12 beslutat att system-ansvariga för verksamhetssystem samt administrativ chef inom barn- och ungdomskontoret utses till personuppgiftssamordnare för barn- och ungdomsnämnden.

Samhällsbyggnadsnämnden, SBN, har 2018-11-03 beslutat att ge samhällsbyggnadskontorets chef i uppdrag att utse personuppgiftssamordnare för samhällsbyggnadsnämnden. GIS-samordnaren är utsedd till personuppgiftssamordnare, beslutet finns dock inte formaliserat, men denne kommer att sluta sin tjänst i augusti 2019. Arbetet med att utse en eller flera personuppgiftssamordnare för samhällsbyggnadsnämnden pågår. Samhällsbyggnadskontoret består av fem olika verksamheter; plan- och byggenheten, miljöenheten, kostenheten, park, gatu- och lokalvårdsenheten samt VA- och renhållningsenheten som alla arbetar i olika verksamhetssystem varför flera personuppgifts-samordnare bör utses.

Kommunstyrelsen, KS, i Hylte kommun har 2018-10-09 beslutat att informationssäkerhets-samordnare på informations- och kanslienheten, löne-och systemansvarig på personalenheten, systemansvarig på ekonomienheten samt säkerhetssamordnare på räddningstjänsten utses till personuppgiftssamordnare för kommunstyrelsen

Valnämnden, VN, har inte utsett en personuppgiftssamordnare utan följer kommunstyrelsen. Kommunstyrelsen i Hylte kommun har 2018-10-09 beslutat att informationssäkerhetssamordnare på informations- och kanslienheten, löne-och systemansvarig på personalenheten, systemansvarig på ekonomienheten samt säkerhetssamordnare på räddningstjänsten utses till personuppgifts-samordnare för kommunstyrelsen

Tillsynsnämnden, TN, bedriver tillsynsverksamhet över Hylte kommuns verksamheter inom bygg-, miljö- och hälsoskyddsområdet. Nämnden prövar även tillstånd som krävs inom dessa verksamheter. Syftet är att en fristående nämnd ska granska kommunens verksamheter inom dessa områden för att förhindra att de enskilda nämnderna bedriver tillsyn eller ger tillstånd åt sina egna verksamheter.

Tillsynsnämnden har inte fattat beslut om att utse någon personuppgiftssamordnare eller registerförtecknare. Nämndsekreteraren har agerat registerförtecknare för viss form av dokumentation/diarieföring. Tillsynsnämnden och samhällsbyggnadsnämnden är nära samman-kopplade och arbetar under samma verksamhet. Tillsynsnämnden hanterar personuppgifter vid tillsyn av samhällsbyggnadsnämnden. Ett förslag är att tillsynsnämnden tar ett generellt beslut att följa samhällsnämndens beslut om personuppgiftssamordnare.

Bostadsstiftelsen Hyltebostäder har utsett en och samma person till registerförtecknare och personuppgift-samordnare.

3.2. Har kommunen en utpekad, centralt placerad, samordnande roll för kommunens totala informationssäkerhetsarbete?

Hylte kommun har en anställd informationssäkerhetssamordnare sedan mars månad år 2019 och rollen har ett övergripande ansvar för informationssäkerhetsarbetet i hela kommunen.

3.3. Har era personuppgiftssamordnare/motsvarande genomgått någon extern utbildning i GDPR, exempelvis arrangerad av Datainspektionen?

ANN - den före detta PUS för IFO Vuxen har genomgått utbildning. Integrationsenheten har

deltagit i följande kurser – ”Nya dataskyddsförordningen i offentlig sektor”, Offentliga Utbildningar, 2018-02-22 och ”GDPR för socialtjänsten” (webbseminarium), SKL, 2018-03-13.

Övriga personuppgiftssamordnare har inte deltagit i några externa utbildningar. Internt har alla personuppgiftssamordnare samt enhetschefer för arbets- och näringslivsnämnden under år 2018 gått en internutbildning om GDPR, anordnad av kommunens kommunjurist och IT-samordnare.

ON - ingen av personuppgiftssamordnarna eller registerförtecknarna för Omsorgsnämnden har deltagit i någon extern utbildning i GDPR utan har endast deltagit i den interna.

SBN - nuvarande personuppgiftssamordnare har inte genomgått någon extern utbildning.

BUN - ingen av personuppgiftssamordnarna eller registerförtecknarna för Barn och ungdomsnämnden har deltagit någon extern utbildning i GDPR.

KS och **VN** - informationssäkerhetssamordnaren har deltagit i följande kurser i GDPR: ”GDPR - Nya dataskyddsförordningen i offentlig sektor”, Offentliga Utbildningar, 2018-02-22 och ”GDPR för socialtjänsten” (webbseminarium), SKL, 2018-03-13.

Informationssäkerhetssamordnare, övriga personuppgiftssamordnare samt de flesta som gjort registerförteckningar för kommunstyrelsen har år 2018 deltagit i den interna utbildning om GDPR anordnad av kommunens kommunjurist och IT-samordnare.

TN - har ingen utsedd personuppgiftssamordnare.

Bostadsstiftelsen Hyltebostäder – har inte deltagit i någon utbildning.

3.4. Har ni gjort klart er kartläggning av personuppgiftsbehandlingar och upprättat registerförteckningar?

ANN - svarar ja på frågan. Kartläggningar och registerförteckningar är upprättade i Draftit. Vissa punkter behöver eventuellt kompletteras. De flesta förteckningarna över registreringarna för socialtjänsten är gjord. Återkommande kontroller av registreringar ska göras.

ON - registreringen i Draftit är färdig men kommer troligen att fyllas på efterhand. Man även gått igenom all dokumentation som legat under T och rensat/flyttat övervägande dokumentation till Platina.

SBN - registerförteckningar finns i Draftit för verksamhetens centrala system, dock är de i några fall ofullständiga.

BUN - nej. Man har påbörjat registrering på BUK administration. Skoladministratörerna skulle få info och hjälp ute på enheterna av kommunansvarig under våren 2018, tyvärr blev det inte så. Istället blev det en gemensam förkortad informationsträff och därefter inget mer. Någon administratör har säkert påbörjat registrering men arbetet är långt ifrån färdigt.

55 st. registreringar är gjorda i Draftit för BUK-administrationen och innefattar de stora systemen som används inom BUK. Ingen enhet/skola har gjort några registreringar.

KS – det ser olika ut på respektive enhet/funktion.
Information/kansli (kommunikation, kommunadministration, Kontaktcenter), IT, Personal, Räddningstjänst - registerförteckningar i Draftit är upprättade för i stort sett all den behandling av personuppgifter som man gör. Dock anser man att lämnad information behöver kontrolleras och följas upp.

Ekonomi - har gjort en registrering i Draftit och har meddelat att man inte har genomfört flera på grund av hård arbetsbelastning under 2018. Enheten är nu fulltalig och arbetet med registreringar kan påbörjas igen.

Digitaliseringsenheten - är en ny enhet som kan behöva stöttning i att påbörja arbetet med Draftit. Mycket av den personuppgiftsbehandling de hanterar har funnits fördelad på andra funktioner inom KS, så registreringar kan vara gjorda för enheten. Behöver kontrolleras och följas upp.

VN - nämndsekreterare/valsamordnare har agerat registerförtecknare för viss form av dokumentation/diarieföring

TN - registerförteckningar genomförda av samhällsbyggnadsnämnden finns i Draftit för den centrala verksamhetens system, dock är i de några fall ofullständiga. Tillsynsnämnden använder samma centrala system men någon registrering för deras behandling är inte gjord. Nämnd-sekreterare har agerat registerförtecknare för viss form av dokumentation/diarieföring för nämnden.

Bostadsstiftelsen Hyltebostäder - i Draftit finns 16 registreringar. Inga nya registreringar är gjorda under 2019.

3.5. Har ni identifierat era personuppgiftsbiträden och tecknat biträdesavtal?

ANN har identifierat biträdena för Örnahallen Hälsocenter, Hylte Fritidsgård och Mobil Fritidsgård. Detsamma gäller för IFO Vuxen och för biblioteksverksamheten. Dessa biträden finns även registrerade i Draftit. AME har också identifierat sina personuppgiftsbiträden. Men person-uppgiftsbiträdesavtal är inte på plats för alla personuppgiftsbiträden inom ANN.

För bibliotekssystemet finns personuppgiftsbiträdesavtal samt för vissa digitala tjänster. Hyltebiblioteken använder som e-bokstjänst Elib och Simplesignup som används vid anmälan till evenemang. För AME.s och ESF-projektet Integration Hallands ärendehanteringssystem (GW Arbetsmarknad och Accorda) finns personuppgiftsbiträdesavtal. Personuppgiftssamordnaren för fritid-och folkhälsa håller på att upprätta ett biträdesavtal med hjälp av kommunens informationssäkerhetssamordnare.

ON – delvis. En del personuppgiftsbiträdesavtal finns på plats för de stora leverantörerna som CGI.

SBN – de är identifierade till viss del och det finns några enstaka personuppgiftsbiträdesavtal på plats.

BUN - några av dem är identifierade genom våra avtal, licenser och system och med vissa finns biträdesavtal, främst där det har tecknats nya avtal eller om det är stora systemleverantörer.

KS - personuppgiftsbiträden är identifierade till de stora verksamhetssystemen men även här behöver man se över de registreringar som är gjorda så man inte missar att registrera nya och små system. I vissa fall har man svarat att man har personuppgiftsbiträden men inte namngett dem i Draftit. I många fall där man identifierat personuppgiftsbiträden har men inte biträdesavtal på plats. Det finns fyra PUB-avtal diarieförda för KLK. Enligt registreringarna i Draftit så är 9 stycken olika biträden identifierade som hanterar personuppgifter. Enligt interna listor över verksamhetssystem så finns det 28 stycken system som används på KLK idag. En kontroll behöver göras för att se i vilka av dessa system man behandlar personuppgifter. Anledningen till att fler biträdesavtal inte finns registrerade uppges vara allt ifrån att man har skickat avtal men inte följt upp om de har kommit tillbaka, till att man inte vetat hur avtalen skulle utformas eller vem som skulle hålla i upprättandet av avtalen

VN - personuppgiftsbiträden är identifierade till de stora verksamhetssystemen men även här behöver man se över de registreringar som är gjorda så man inte missar att registrera nya och små system. I vissa fall har man svarat att man har personuppgiftsbiträden men inte namngett dem i Draftit. Valkansliets arbete dokumenteras och diarieförs i verksamhetssystemet Platina, det finns inget biträdesavtal upprättat med leverantören Formpipe.

TN – biträdena är identifierade till viss del för samhällsbyggnadsnämnden. Tillsynsnämnden har samma. Det finns några enstaka personuppgiftsbiträdesavtal för samhällsbyggnadsnämnden. Tillsynsnämnden har samma.

Hyltebostäder - här har man angett sina PUS. Man har inte identifierat biträdesavtal.

3.6. Har ni en fastställd rutin/process för uppdatering och uppstart av nya personuppgiftsbehandlingar?

ANN - nej, det finns inte. Riktlinjer för hantering/registrering av personuppgifter finns men det finns ingen kännedom om en specifik rutin/process för uppdatering eller uppstart av nya person-uppgiftsbehandlingar, mer än rutinen för registrering i Draftit.

För bibliotekens del är den under framtagande. Kontroll av registreringar bör göras allt eftersom verksamheten utvecklas och arbetssätt förändras, för bibliotekens del är den snabba digitala utvecklingen en viktig faktor.

ON - nej

SBN - nej.

BUN - vet inte, tror inte det. Inte för BUK specifikt utan det är om det finns någon för Hylte kommun.

KS, VN - nej, det finns ingen fastställd rutin eller process för kommunstyrelsen gällande uppdatering/uppstart av personuppgiftsbehandlingar

TN - nej.

Hyltebostäder - nej.

3.7. Har ni en fastställd process för begäran om registerutdrag?

ANN - nej. Alla låntagare har rätt att få utdrag ur vårt bibliotekssystem KOHA när de legitimerat sig.

ON – nej.

SBN – nej.

BUN - ja, den som finns hos Hylte Kommun vid anställning. Tyvärr ser vi brister här då den inte alltid följs. Vikarier måste lämna in utdrag ur belastningsregistret innan de får stå med på vikarielistan.

För möjligheten till registerutdrag enligt GDPR så finns det ingen fastställd process för det.

KS och VN – nej, det finns ingen fastställd process för registerutdrag enlig GDPR. Registerutdrag efterfrågas ibland inom de olika verksamheterna men det finns ingen nedskriven rutin. En sådan

förfrågan hanteras genom att man sökt efter personen som begärt ut handlingen i samtliga verksamhetssystem (för den enheten) och skrivit ner och meddelat vad man eventuellt hittat.

TN - nej.

Hyltebostäder - Kan vi använda samma rutin som vi har för utlämnande av handlingar?

3.8. Har ni en fastställd rutin för incidenthantering/incidentrapportering?

ANN, ON, SBN, BUN, TN, Hyltebostäder, KS och VN – svarar samstämmigt nej, men kommunen har en digital e-lösning för incidentrapportering som ännu inte är i bruk. Organisationen runt incidenthanteringen samt rutiner och liknande är inte klara och därför har lösningen inte introducerats på intranätet.

3.9. Behandlar ni särskilda kategorier av personuppgifter?

ANN - ja, bl.a. hälsouppgifter i samband med hälsoprofilsbedömningar genom Uppdrag Hälsa och Integration Halland samt registreringar med känsliga personuppgifter från IFO Vuxen och f.d. Integrationsenheten. Den enda uppgift som registreras i biblioteksystemet som kan vara känslig, är om en låntagare är ”talbokslåntagare” vilket man kan vara av olika anledningar men som inte specificeras vid registrering. För att bli Talbokslåntagare får man skriva på ett speciellt avtal om att man godkänner att uppgifterna lagras om att man är Talbokslåntagare.

ON – ja, känsliga personuppgifter i form av hälsouppgifter i patientjournaler samt myndighetsuppgifter. De förvaras i verksamhetssystem och dokumenthanteringsprogrammet Platina.

SBN – ja, ekonomiska uppgifter samt uppgifter som rör personers anställning behandlas.

BUN – nej (m.a.o. är svaret ja), inte annat än i systemet Heroma och gällande sjukskrivningar.

Inom skolan hanteras en stor mängd känsliga personuppgifter i olika sammanhang. Det kan vara att man i skolans dagliga verksamhet måste ta hänsyn till hälsoinformation men det kan också vara vid tillbud, olyckor och kränkningar som känsliga personuppgifter hanteras i dokumentation och liknande. Även inom IFO Barn och unga hanteras känsliga personuppgifter i stor utsträckning i det dagliga arbetet.

KS - inom de olika verksamheterna hanteras känsliga personuppgifter främst i form av hälso-uppgifter och facklig tillhörighet (personal, ekonomi) men även kommunsekreterarna hanterar

känsliga personuppgifter och i vissa fall görs det även det inom de andra enheterna. Personnummer hanteras inom alla enheterna.

VN - nej, men personnummer behandlas. Känsliga personuppgifter så som etnicitet osv kan komma att behandlas under röstningsregistrering. Dessa uppgifter finns i ett nationellt valdatabassystem som upprättas av Valmyndigheten, där bland annat uppgifter om rösträtt finns. Behörigheten är tillfällig och begränsad till valperioden och endast ett fåtal inom valkansliet har tillgång.

TN - ekonomiska uppgifter samt uppgifter som rör personers anställning på samhälls-byggnadskontoret vid redovisning av delegeringsbeslut samt hälsouppgifter och ekonomiska uppgifter som en följd av samhällsbyggnadskontorets verksamhetsarbete.

Hyltebostäder - nej.

3.10. Om ni svarat att ni behandlar särskilda kategorier personuppgifter, har ni gjort en konsekvensbedömning för behandlingen?

ANN - inte ännu. En konsekvensbedömning för HPB (Uppdrag Hälsa) är påbörjad av PUS på fritid- och folkhälsa med kommunens säkerhetssambordnare.

ON, **SBN, BUN**, **KS, VN, TN och Hyltebostäder -** nej.

3.11. Har er nämnd/styrelse en lösning på plats för att digitalt kunna kommunicera känsliga personuppgifter och sekretessbelagd information?

ANN - nej. Dock finns Platina som en lösning till intern kommunikation.

SBN – nej, finns ingen lösning idag

ON - merparten av kommunikationen internt sker via vårt verksamhetssystem där inloggnings-uppgifter krävs och där styrningen sker via behörigheter. Mellan nämnder/verksamheter finns delvis ett digitalt stöd för överföring av kommunikation, via Platina

BUN – nej, vi efterfrågar säker e-post men har fått till svar att det inte finns i Hylte Kommun än. Vår verksamhet är i stort behov av att kunna skicka säker epost då vi skickar mycket personnummer för hantering av betyg, fakturor, inskrivningar i våra verksamheter m m.

KS - för intern kommunikation finns verksamhetssystemet Platina att använda. Alla medarbetare i kommunen med tillträde till admininstratörsnätet har tillgång till Platina. Dock så har inte alla medarbetare ett konto upprättat. Det råder också en stor osäkerhet ute bland medarbetarna om hur man arbetar i Platina och många är sällananvändare.

Inom kommunstyrelsens verksamheter arbetar man med Platina i stort sett dagligen och det är även genom verksamhetssystemet man främst delar information. Det har dock framkommit i samband med denna granskning att vissa verksamheter inom KS använder sig av mail för att dela person-uppgifter i ”krypterad” form, födelseår eller initialer vid interna kontakter och i vissa sammanhang dossier nr och initialer vid kontakt med andra myndigheter/kommuner osv.

För extern kommunikation finns det i dagsläget ingen säker digital lösning. Kommunen har tillgång till Trusted Dialog men man saknar en användarautentiseringslösning (IdP).

VN - för intern kommunikation finns verksamhetssystemet Platina att använda. Alla medarbetare i kommunen med tillträde till admininstratörsnätet har tillgång till Platina. Dock så har inte alla medarbetare ett konto upprättat. Kontakt med Valmyndigheten och Länsstyrelsen sker via telefon.

TN - finns ingen lösning idag.

Hyltebostäder – nej, men vår administrativa enhet skriver aldrig fullständiga namn eller personnr i mail.

3.12. Har er nämnd/styrelse en lösning för att säkerställa säkra utskrifter av dokument?

ANN, ON, SBN, BUN, KS, VN och TN - alla nämnder i kommunen har ”Follow Me Print” i merparten av sina verksamheter. Med "Follow Me" nås full sekretess genom att inga dokument skrivs ut förrän användaren har bestämt det och är på plats vid skrivaren. Genom att logga in får användaren access till sin egen utskrifts kö och kan därifrån fritt välja vilket eller vilka dokument som ska skrivas ut. Inloggningen kan ske genom kort, kod eller tag. Inloggningen kan synkroniseras med företagets befintliga AD (Active directory).

Hyltebostäder - nej.

3.13. Har ni en plan för hur nämnden/styrelsen ska kunna upprätthålla ett långsiktigt arbete kring personuppgiftsbehandling och dataskydd?

ANN - nej, det finns ingen plan men nu när en informationssäkerhetssamordnare finns på plats och PUS är utsedda så kommer det förhoppningsvis att hända mer saker.

ON - nej.

SBN - i första hand ska ny personuppgiftssamordnare utses samt eventuellt registerförtecknare. Kontoret är i behov av att gå igenom de behandlingar som är registrerade i Draftit och komplettera där så behövs. Övriga behandlingar ska identifieras och registreras. Det finns behov av utbildning/ genomgång av GDPR och hur kontoret ska arbeta för att säkerställa att lagstiftningen följs. Rutiner m m bör tas fram på central nivå och kan därefter behöva anpassas efter samhällsbyggnads-nämndens behov. Rutiner och processer ska göras kända inom hela kontoret.

BUN – nej, barn- och ungdomsnämnden har inte någon egen plan för detta

KS och **VN** - nej kommunstyrelsen har inte någon egen plan för detta men med en informationssäkerhetssamordnare på plats så hoppas man att arbetet med bland annat GDPR ska kunna framskrida i en snabbare takt. Valkansliets arbete är väl reglerat genom vallagen och instruktioner från Valmyndigheten och Länsstyrelsen.

TN - i första hand ska ny personuppgiftssamordnare utses samt eventuellt registerförtecknare. Samhällsbyggnadskontoret är i behov av att gå igenom de behandlingar som är registrerade i Draftit och komplettera där så behövs och även se till att tillsynsnämndens är en del av detta arbete. Övriga behandlingar ska identifieras och registreras. Det finns behov av utbildning/genomgång av GDPR och hur kontoret ska arbeta för att säkerställa att lagstiftningen följs. Rutiner m m bör tas fram på central nivå och kan därefter behöva anpassas efter tillsynsnämndens behov. Rutiner och processer ska göras kända inom hela kontoret.

Hyltebostäder - nej.

3.14. Finns det en i er kommun samordnad och tydlig process för hur upphandling av IT-system/tjänster ska gå till?

ANN, ON, SBN, BUN, KS, VN och TN – i Hylte kommun finns det inte en specifik process för hur upphandling av IT-system/tjänster ska gå till men det finns två olika processer som tillsammans bildar en grund för hur en upphandling kan gå till:

”Process för införande av nya system” (se bilder 1a – 1d nedan i avsnittet 3.15) beskriver gången från att ett behov av ett nytt IT-system/tjänst har identifierats ute på en verksamhet och hur processen sedan ser ut i olika steg från behovsanalys och godkännande av ledning till upphandling, införande och drift. Processen är under utveckling och inte ännu antagen.

Som en delprocess finns ”Upphandlingsprocessen” (se bild 2 nedan i avsnitt 3.15) med tillhörande rutiner och avtal och som är antagen. Upphandlingsprocessen finns beskriven på kommunens intranät så alla medarbetare har tillgång till den.

Hyltebostäder - vet inte då det är upphandlingsenheten på kommunen som sköter detta tillsammans med kunnig personal på Hylte kommun.

3.15. Om en process finns, är det i den även uttryckt vilka roller som deltar och vilka deras uppgifter är?

ANN, ON, BUN, SBN, KS, VN och TN - i Hylte kommun finns det inte en specifik process för hur upphandling av IT-system/-tjänster ska gå till men det finns två olika processer som tillsammans bildar en grund för hur en upphandling kan gå till:

”Process för införande av nya system” (se bilder 1a – 1d nedan) beskriver gången från att ett behov av ett nytt IT-system/tjänst har identifierats ute på en verksamhet och hur processen sedan ser ut i olika steg från behovsanalys och godkännande av ledning till upphandling, införande och drift. Processen är under utveckling och ännu inte antagen.

Som en delprocess finns ”Upphandlingsprocessen” (se bild 2 nedan) med tillhörande rutiner och avtal som är antagen. Upphandlingsprocessen finns beskriven på kommunens intranät så alla medarbetare har tillgång till den.

Roller och uppgifter

Process för införande av nya system – roller	**Upphandlingsprocessen - roller**
Objektägare	Nämnd/ledning/chef - firmatecknare
Objektledare	Processledare
Objektspecialist	
	Arbetsgrupp
IT	Upphandlingsfunktion/upphandlare
IT-service	
Leverantör	Leverantör

Roller och uppgifter i processerna:

- *Objektägare* motsvarar ledning eller chef, vars uppgift är att besluta om att inleda eller inte inleda en process för införande av ett nytt IT-system/-tjänst. I slutet av införandeprocessen är det också objektägaren som i samråd med övriga roller, fastställer förutsättningar för driften, (bild 1a och 1d).

  I en upphandlingsprocess är det ledning/chef som står som beslutsfattare i *anskaffningsbeslutet* och bestämmer vilka som ska sitta med i en *arbetsgrupp* för införandet av ett nytt system/ tjänst. Ledning/chef är också delaktiga när

upphandlingsdokumentet utformas samt när beslut fattas om vilken leverantör som tilldelas uppdraget. Avtal signeras av firmatecknare. (Bild 2)

- *Objektledare* motsvarar verksamheten som representeras av en eller flera utsedda professioner, exempelvis systemförvaltare eller *processledare*. Ofta har objektledaren det övergripande ansvaret och är den som inleder och upprätthåller kontakt med övriga roller i processerna.

  Införandeprocessen inleds när ett behov av ett nytt system klargörs av objektledaren *(behovsanalys),* vilket ligger till grund för objektägarens beslut att gå vidare eller inte. Ibland behövs även en *förstudie*, vilket objektledaren i samråd med exempelvis IT upprättar (bild 1a).

  När ett beslut är fattat upprättar objektledaren ett *ärende* hos *IT-service* (bild 1b) och startar upphandlingsprocessen (bild 2). Först kontrollerar objektledaren/processledaren om avtal redan finns, eller om ett *direktköp, direktupphandling* eller en *upphandling* måste ske. Ett *anskaffningsbeslut* tas fram som beskriver vad som ska upphandlas och *upphandlarna* kopplas in. I processledarrollen ingår att kontrollera *upphandlingsdokumentet* innan annonsering, att tillsammans med *arbetsgrupp* besvara frågor och utvärdera inkomna anbud samt fatta beslut om vilken leverantör som får uppdraget, *tilldelningsbeslut.*

  Vidare vid införandet av ett IT-system/-tjänst är det även *objektledarens* roll att *testa* systemet och *godkänna leveransen* (bild 1d).

- *Objektspecialist* är den eller de professioner i en verksamhet, exempelvis systemförvaltare eller processledare som innehar mest kunskap om de olika verksamhetssystemen som används.

- En *Arbetsgrupp* ska alltid tillsättas vid en upphandling och kan bestå av medverkande från flera olika verksamheter i kommunen. Arbetsgruppens syfte är att få in sakkunskap och erfarenhet om produkten/tjänsten som ska upphandlas. Arbetsgruppens uppdrag är att ta fram en kravspecifikation, vad krävs av produkten/tjänsten, och utvärderingskriterier, hur anbuden ska utvärderas. Under upphandling gäller sekretess och är upphandlingen av stort värde ska även ekonomienheten kopplas in för att säkerställa koncernnyttan.

- *Upphandlarna* är den funktion i kommunen som förbereder upphandlingar genom förstudier/ analyser samt följer upp genomförda upphandlingar. Har en rådgivande roll åt verksamheterna i upphandlingsfrågor och deltar i förhandlingar, utformar kontrakt och förvaltar ingångna avtal.

- *IT* finns med under hela införandeprocessen och även i upphandlingsprocessen är det viktigt att IT representeras i *arbetsgruppen* för att en hållbar kravspecifikation ska kunna upprättas.

  Under den inledande införandeprocessen fungerar IT som ett stöd för objektledaren och är involverad i en eventuell *förstudie.* Kontroller görs om det är möjligt att genomföra införandet i befintliga IT-system och vilka valmöjligheter som finns osv. (Bild 1a).

  När upphandlingen är genomförd så hålls ett *uppstartsmöte* med IT, *IT-service* och leverantören för att påbörja själva den tekniska installationen av ett system eller tjänst (bild 1c). Tester och liknande genomförs tillsammans med *objektledare* och *IT-service.* När systemet/tjänsten väl är i drift så gör IT en utvärdering av systemet och processen (bild 1d).

- *IT-service* är i Hylte kommun den IT-partner kommunen har ett outsourcingavtal med för att sköta IT-driften. I införandeprocessen får de ett *ärende* av objektledaren när upphandlingsprocessen påbörjas, och förbereder under upphandlingen inför ett *uppstartsmöte* när leverantör väl är beslutad. Tillsammans med IT och leverantör genomför de sedan den tekniska installationen. Det är också IT-service som efter direktiv av objektägaren sköter underhåll för den fortsatta driften. (Bild 1a – 1c).

- *Leverantör* är det företag som levererar det IT-system/-tjänst som verksamheten är i behov av. Leverantörer lämnar anbud under upphandlingsprocessen (bild 2) och om man blir tilldelad uppdraget så påbörjas samarbetet med de olika rollerna i införandeprocessen under *uppstartsmötet*. Leverantörens främsta samarbetspartner i införandeprocessen är IT-service.

Bild 1a - process för införande av nya system

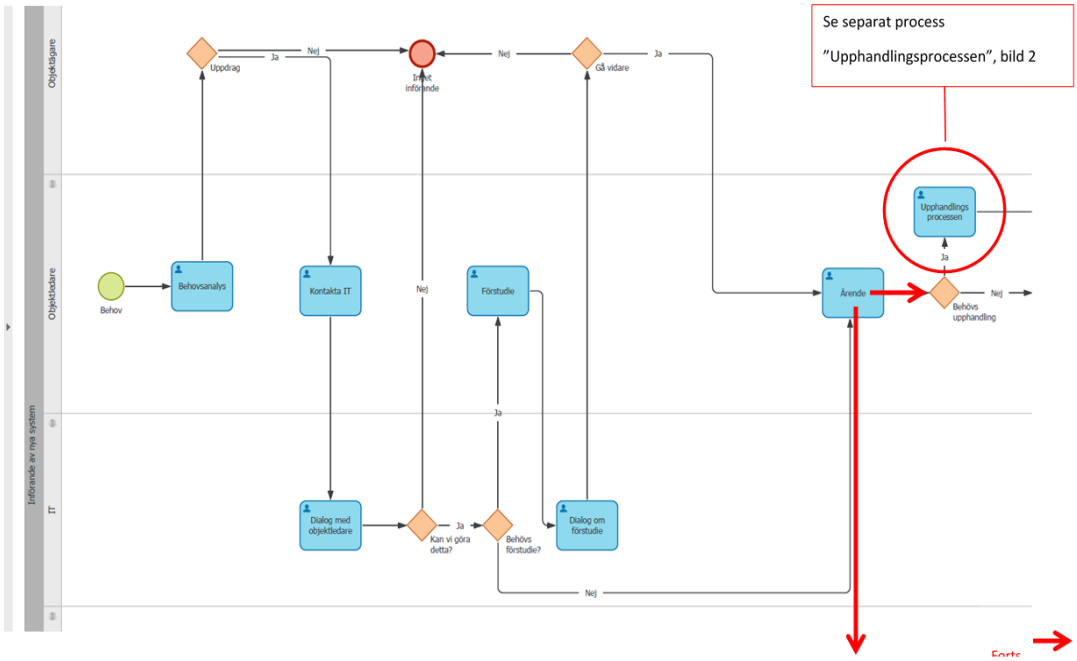


Bild 1b - process för införande av nya system

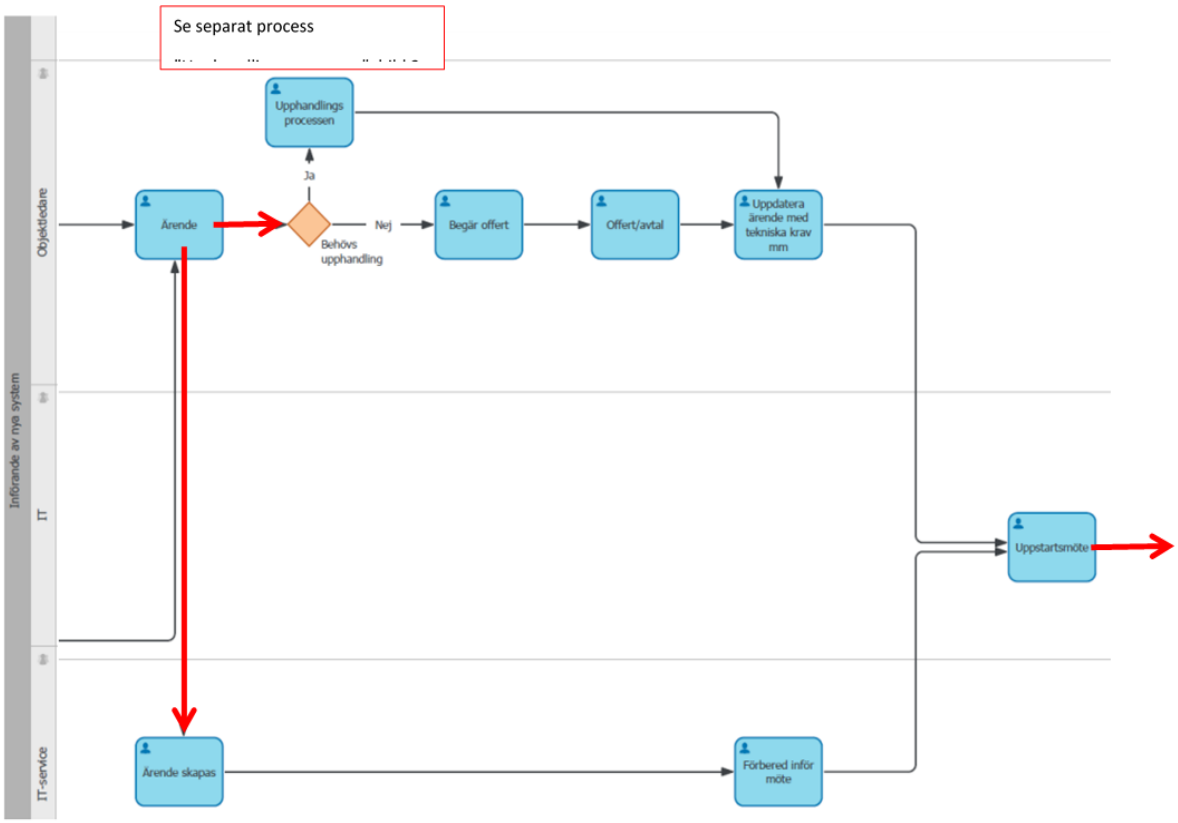


Bild 1c - process för införande av nya system

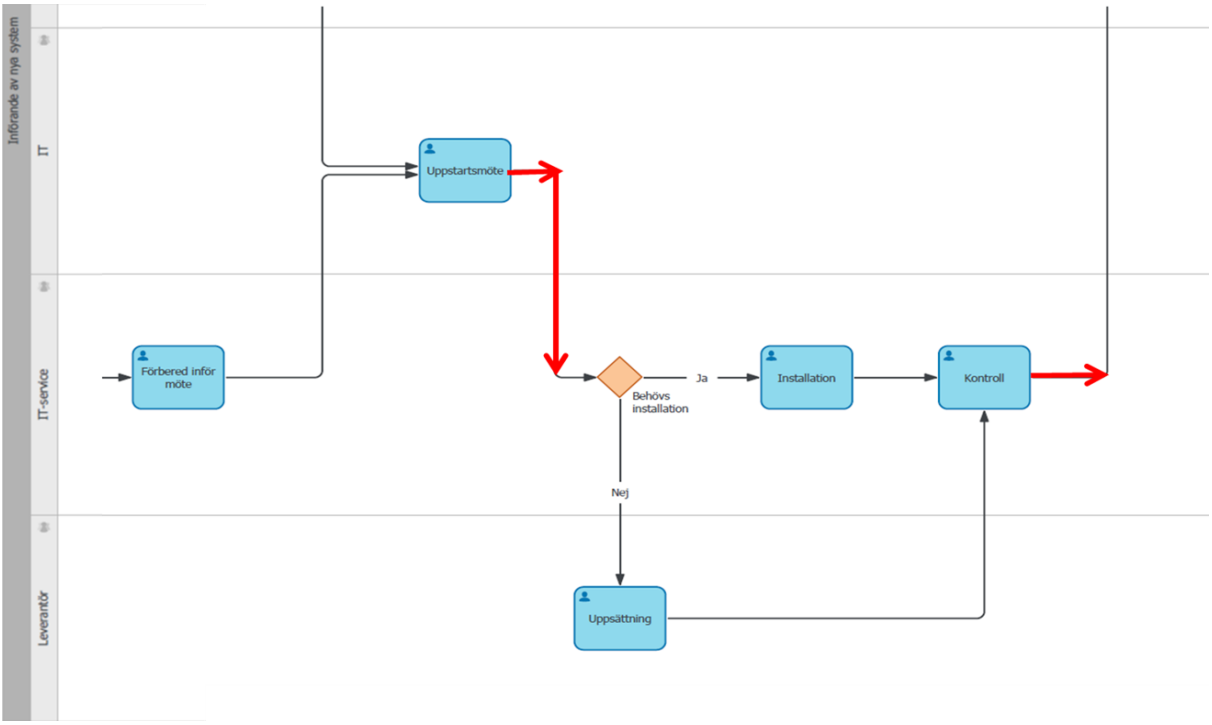


Bild 1d - process för införande av nya system

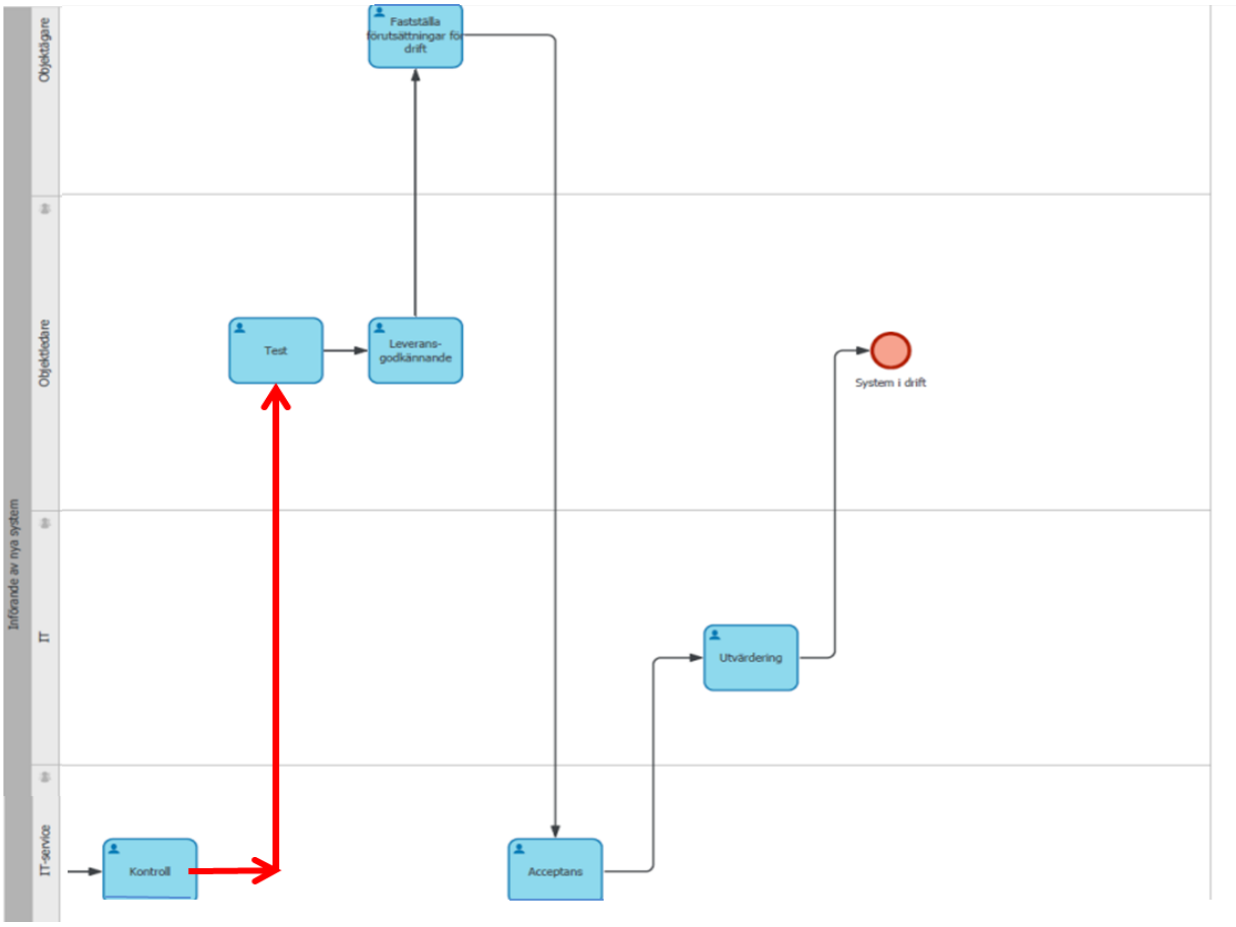
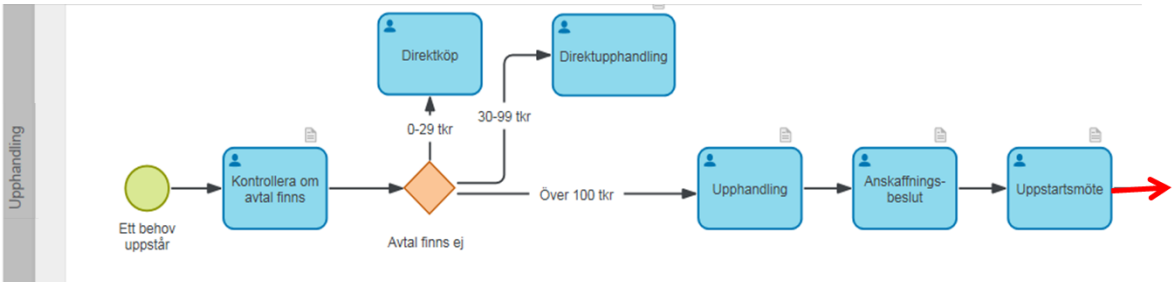
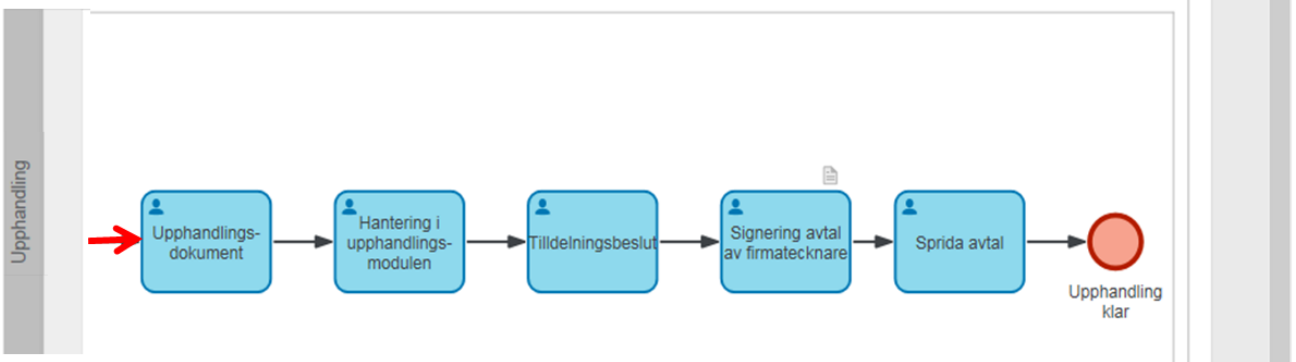


Bild 2 – upphandlingsprocessen

a) *Avtal* kontrolleras i avtalsbas på intranätet, *direktköp* kostnad lägre än 30 tkr/ 4 år, *direktupphandling* 30- 100 tkr/ 4 år, om *upphandling* behövs ska policy och riktlinjer för ”upphandling och inköp” följas, ett *anskaffningsbeslut* fylls i, upphandlare kallas till *uppstartsmöte* för att diskutera strategi.



Upphandlingsdokument beskriver vad som ska upphandlas och ska utannonseras, *hantering* frågor och svar hanteras skyndsamt, utvärdering under strikt sekretess av inkomna anbud, *tilldelningsbeslut* fattas av processledare, *signeraring av avtal* sker genom firmatecknare om kostnas över 100 tkr., *sprida avtal* genom att lägga in i avtalskoatalog och meddela berörda enheter.



4. Analys, diskussion och slutsats

I detta avsnitt analyseras och diskuteras inkomna svar från nämnderna och styrelserna på utskickat frågeunderlag. Här ges även råd och rekommendationer under avsnitten slutsatser.

4.1. Rollen PUS är utsedd i de flesta nämnder och styrelser

I ett beslut från Hylte kommuns (dnr 2018 KS0199) kommunstyrelse följer att; ”Styrelser och nämnder ska utse personuppgiftssamordnare för att ansvara för och samordna personuppgifts-behandlingen i det operativa arbetet. De som utses som personuppgiftssamordnare ska vara en kontaktperson till dataskyddsombudet.”

En grundläggande förutsättning för att verksamheterna ska kunna leva upp till GDPRs krav, det är att det finns ansvariga roller utpekade för det praktiska arbetet t ex personuppgiftssamordnare. Dessa personer måste få avsatt tillräckligt med tid för uppgifterna och ha kompetens inom GDPR men också i den egna verksamhetens specifika lagar. Det är viktigt att personuppgiftsansvariga, chefer och ledningspersoner är väl insatta i vad dessa roller innebär i omfattning och kompetens.

Hylte kommun har inte tagit ett beslut om att nämnderna även ska utse registerförtecknare, RF. Det har Falkenbergs och Laholms kommuner beslutat om att utse. Om man behöver utse registerför-tecknare så är det upp till verksamheterna att göra det. Många av de utsedda personuppgifts-samordnarna i Hylte kommun hanterar de uppgifter som annars ligger på rollen registerförtecknare alternativt att uppgiften ligger på systemadministratörerna.

Ansvariga och drivande i arbetet med anpassningen av kommunens personuppgiftshantering till den nya lagstiftningen var kanslichefen på kommunstyrelsens förvaltning Susanne Mared, IT-samordnaren Hanna Arvidsson och kommunjuristen Anna Hedqvist. De har med begränsade resurser bl. a vad gäller tid, lyckats driva arbetet framåt i nämnder och styrelser.

Det är nästan ett måste att ha flera personuppgiftssamordnare utsedda inom varje nämnd, speciellt om det är en stor verksamhet och/eller om den består av många olika typer av verksamheter.

Arbetslivs- och näringslivsnämnden, AN, har utsett en PUS för respektive verksamhet och att utse en för varje verksamhet är ett utmärkt upplägg. Då får man personer som är väl insatta i just de verksamhetsspecifika personuppgiftsbehandlingarna istället för att en PUS ifrån en helt annan verksamhet ska sätt sig in i behandlingarna.

I svar från Samhällsbyggnadsnämnden, SBN, anger man att arbetet pågår med att utse en PUS för respektive verksamhet vilket som sagts tidigare, är ett väldigt bra upplägg.

Tillsynsnämnden är den enda nämnd där man inte utsett någon PUS men nämndsekreteraren har varit informellt ansvarig för frågorna. Lämpligt är att nämnden även formellt utser rollen PUS.

Slutsatser
Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör**;**

- säkerställa att rollen PUS för respektive nämnd/styrelse finns på plats, t ex inom Tillsynsnämnden och Samhällsbyggnadsnämnden som angett att man inte har sådan på plats
- verka för att de nämnder som är stora och har en bredd i sin verksamhet utser en PUS för varje verksamhet alt flera PUS inom sin nämnd om den är stor
- överväga att utse RF, speciellt inom de nämnder som är stora och breda i sin verksamhet. Utser man inte RF är det särskilt viktigt att man tydliggör vem som ansvarar för att praktiskt upprätta registerförteckningar
- bli väl insatta i vad rollerna PUS och RF innebär, vilka uppgifter de har och vilken omfattning i tid som krävs

4.2. Kommunen har en samordnare för kommunens totala informationssäkerhetsarbete

Hylte kommun är en av de kloka kommuner som prioriterat att ha en anställd samordnare för kommunens totala och övergripande arbete med informationssäkerhet. Sedan mars år 2019 har man en heltidsanställd samordnare på plats. Det är en oerhört viktig roll att ha på plats och den är en grundförutsättning för att kunna bedriva ett systematiskt informationssäkerhetsarbete.

Generellt så är behovet av att arbeta systematiskt med informationssäkerhet och person-uppgiftsskydd hos myndigheter och företag i Sverige oerhört stort. Det visar återkommande rapporter från bl. a Myndigheten för Samhällsskydd och Beredskap, MSB. Bara de senaste åren har det dessutom kommit många nya lagar förutom GDPR, t ex säkerhetsskyddslagen och NIS-direktivet. Dessa regelverk ökar kraven på hur information ska hanteras. Dessutom har antalet risker för diverse angrepp som virus, sabotage och bedrägerier ökat drastiskt mot företag och organisationer och det i takt med den ökade digitaliseringen.

Kommuner, övriga myndigheter och organisationer måste ha kunskap om vilken typ av information de hanterar - vilken typ av information man har och varför, var den finns, vilka IT-system som används, vem som har behörighet och hur viktig den är för kommunen ur perspektiven till-gänglighet, konfidentialitet och riktighet. Att ha kontroll över allt detta utgör grunden för att kunna utveckla arbetsprocesser med digitaliseringens hjälp och för att kunna ge informationen rätt skyddsnivå både ur ett tekniskt perspektiv och utifrån juridiska krav.

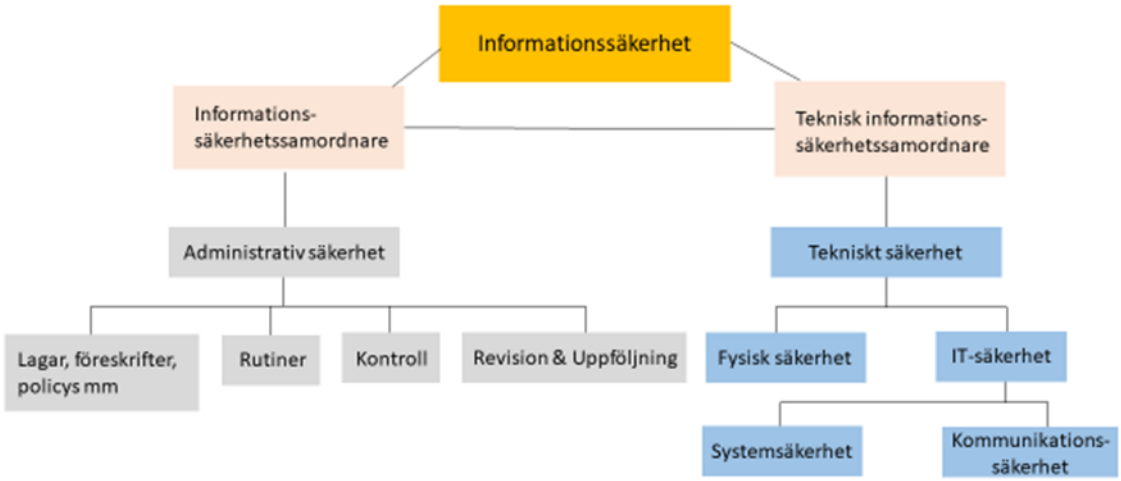
En kommun är ju helt beroende av sin information – både den som kommer in och den som upprättas inom kommunen. Information, både i digital och analog form, finns i mängder. Den finns i diverse verksamhetssystem, på webbplatser, på intranät, i traditionella arkiv osv. Alla verksamheter inom kommunen hanterar information som nämndprotokoll, beslutsunderlag, avtal, organisationsbeskrivningar, ansökningar, kartor, ritningar, socialutredningar gällande barn,

uppgifter om hälsa, uppgifter om elnät och vattenförsörjning, fakturor, bilder m m. Tänk om hemtjänstens eller socialtjänstens IT-system skulle slås ut eller att någon gör ett intrång i systemen och ändrar i informationen? Det skulle kunna utgöra fara för liv och hälsa. Eller tänk om underlagen till socialnämndens beslutsärenden är manipulerade? Eller helt enkelt raderade? Konsekvenserna kan bli förödande både för den enskilde och samhället i stort. Och sist men inte minst skulle förtroendet för kommunens verksamhet allvarligt skadas.

Medarbetare, förtroendevalda och enskilda måste kunna vara trygga med att kommunens information är tillgänglig när den behövs, att den är korrekt och inte manipulerad, att information som är känslig inte kan nås av obehöriga och att det finns tekniskt skydd och lösningar till hjälp för att kunna förhindra och spåra skador på informationen i form av dataintrång, spridning av skadlig kod osv.

Informationssäkerhetsarbetet måste bedrivas utifrån både ett administrativt säkerhetsperspektiv och ur ett tekniskt säkerhetsperspektiv. Rollen informationssäkerhetssamordnare finns på plats men det är också bra att ha en utpekad ansvarig roll för den tekniska informationssäkerheten. De medarbetare som arbetar med IT och som finns på kansli- och kommunikationsenheten har hög kompetens både vad gäller informationssäkerhet och teknisk säkerhet. Dock är det alltid bra att tilldela någon person det specifika ansvaret för frågorna.

De olika delarna i informationssäkerhetsarbetet kan illustreras enligt nedan;



Slutsatser
Berörda personuppgiftsansvariga nämnder, styrelser, chefer och ledningspersoner bör;

- verka för att tilldela en specifik person ansvaret för de tekniska informations-säkerhetsfrågorna.

4.3. De flesta av personuppgiftssamordnarna har genomgått en intern utbildning i GDPR

Ett fåtal av personuppgiftssamordnarna har genomgått någon extern utbildning i GDPR. Ett par stycken har gått utbildning i GDPR anordnad av Offentliga Utbildningar och/eller SKLs webbseminarium om GDPR för socialtjänsten. Alla PUS har dock fått en intern utbildning som hölls av kommunjuristen och IT-samordnaren (tillika dåvarande PUS för kommunstyrelsen).

Något som behöver komma på plats i Hylte kommun, det är ett forum/nätverk där samtliga PUS i kommunens nämnder och styrelser regelbundet ses för erfarenhetsutbyte, för information/ utbildning, statusuppdateringar över arbetet inom GDPR och informationssäkerhet, mm. Det kan också vara ett forum där man arbetar fram diverse processer, riktlinjer och instruktioner för personuppgiftshanteringen. Ett nätverk som regelbundet möts är oerhört värdefullt. Kommunens informationssäkerhetssamordnare, tillika PUS för kommunstyrelsen, har planer på att dra igång sådant under våren 2020.

Slutsatser
Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör**;**

- verka för att ett forum/nätverk för kommunens PUS snarast startas upp och som regelbundet träffas för information/utbildning, erfarenhetsutbyte och samarbete inom områdena GDPR och informationssäkerhet
- prioritera anordnandet av utbildningar i regelverket kring informationshantering - GDPR, TF, OSL m.fl. men även utbildning i verksamhetsspecifik lagstiftning då regelverken måste tolkas i beaktande av varandra
- verka för att utbildning/information sker i olika former och gärna på digital väg inom dataskydd/ informationssäkerhet t ex s.k. nano Learning – utbildning inkl. frågor som kanske tar max 5 min/tillfälle och som skickas ut till samtliga anställda i kommunen via e-post under en given tidsperiod

4.4. Verksamheterna har kommit olika långt i sitt arbete med register-förteckningar

Till hjälp för att upprätta registerförteckningar nyttjar samtliga verksamheter i Hylte kommun Draftit IT-stöd.

Bland kommunstyrelsens enheter varierar det i hur långt man kommit med arbetet. Kommun-styrelsens förvaltning bör därför prioritera arbetet inom de enheter där man ligger efter, vilket är inom ekonomi- och digitaliseringsenheterna. Tillsynsnämnden svarar att inga registerförteckningar över behandlingar är gjorda och där bör man snarast kartlägga och förtecknar sina eventuella personuppgiftsbehandlingar.

Nämnderna verkar främst ha registrerat de strukturerade personuppgiftsbehandlingarna som görs i diverse system. Den enda nämnd som specifikt nämner behandlingarna i ostrukturerat material är Omsorgsnämnden och de har gått igenom all dokumentation som legat under deras lagringsyta T. Där har man rensat och även flyttat information till lämpligare lagringsytor som diverse verksamhetssystem. Det är mycket bra att arbeta på det sättet med sina informationsmängder.

Inom Barn- och ungdomsnämnden återstår en hel del arbete. På BUK är arbetet påbörjat men ingen enhet/skola har gjort några förteckningar över sina behandlingar. I svaren till dataskyddsombudet framkommer att skoladministratörerna ute på skolorna blivit utlovade information och hjälp av den som är centralt ansvarig för GDPR-arbetet. Informationsträff genomfördes men sedan fick de ingen mer hjälp. Enligt deras egen uppgift finns PUS utsedda – de utgörs av systemansvariga samt den administrativa chefen. Med PUS på plats så handlar det ju delvis om skapa en struktur för hur arbetet ska bedrivas rent praktiskt inom den egna nämndens verksamhet.

En brist i Hylte kommuns arbete med GDPR, främst efter lagens ikraftträdande, har varit att det inte funnits något kommuninternt nätverk på plats för kommunens PUS att mötas i. Tanken var att sådant skulle startas. Avsaknaden av nätverk har säkert bidragit till oklarheter m m kring arbetet generellt. Orsaken till att inget nätverk kom igång kan delvis förklaras av bristen på personella resurser och på personalomsättning. Det är därför av yttersta vikt att ett sådant nätverk kommer på plats. Nätverket ska vara ett forum för bl. a erfarenhetsutbyte, kompetensöverföring och information.

Slutsatser

Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- verka för att skapa en metod för hur kartläggning av personuppgiftsbehandlingar i ostrukturerat material ska göras
- verka för att ett kommunövergripande nätverk för personuppgiftssamordnare skapas
- fortsätta påbörjade arbete med registerförteckningar

4.5. Det återstår en hel del arbete med att identifiera biträden och teckna biträdesavtal

Av nämnderna och styrelsernas svar att döma kvarstår en hel del arbete med att identifiera biträden och att revidera alternativt teckna biträdesavtal. Kommunstyrelsen svarar att man inte heller vetat hur avtalen ska utformas eller vem som ska hålla i upprättandet av avtalen.

SKL, nu SKR, har en mall som man sedan länge uppmanat kommuner att nyttja för biträdesavtalen. Dataskyddsombudet anser SKRs mall vara för omfattande. SKR borde ta fram varianter och det utifrån de olika ”grader” av biträdesförhållanden som kan råda. Det finns fall då en PUA i princip ”bara” lämnar ut personuppgifter till en extern part till fall då kommunen lagrar all information hos en extern IT-leverantör. Ibland behövs en mycket detaljerad och tydlig styrning från PUAs sida vad gäller PUBs uppdrag, medan det i andra fall räcker med ett enkelt förtydligande av informations-flödena parterna emellan. Många gånger är dessutom verksamheterna oerhört styrda av diverse speciallagar och då finns egentligen inget utrymme för någon av parterna att vara PUA och styra över den andres behandlingar.

Dataskyddsombudet har, tillsammans med bl. a socialförvaltningen i Falkenberg, tagit fram ett utkast till datadelningsavtal avsett att nyttjas i relationen till de privata vårdgivarna. Social-nämndens och de privata aktörernas verksamhet styrs av i princip samma regelverk, t ex PDL, SOL, OSL, HSL m.fl. Därigenom finns små möjligheter för en PUA att ge instruktioner till en PUB hur personuppgifter och information ska hanteras. Enligt SKR ska parterna i dessa lägen nyttja SKRs 13 sidiga biträdesmall vilket både socialförvaltningen och DSO anser i stora delar var i princip omöjlig att använda. Fler och fler DSOer i kommunsverige anser att SKLs mall inte är tillämpbar.

Det finns dock ett annat stort problem vad gäller ev. biträdesrelationer och det är att det har tecknats, och fortfarande tecknas, ett stort antal onödiga biträdesavtal. Det sker delvis för att det i många fall är mycket svårt att utröna vem som är vad i en situation där tjänster delvis utförs av annan part och information delas på diverse sätt. Informationen från SKR och DI genom åren har dessutom alltid varit ganska ”tunn” och helt inriktad på att biträdesavtal i princip alltid ska tecknas så fort det sker någon form av personuppgiftsutbyte. En relativt nya rapport från Svenskt Näringsliv belyser på ett mycket bra sätt komplexiteten gällande biträdesfrågan. De är också av uppfattningen att det måste finnas någon form av enklare datadelningsöverenskommelser mellan parter som delar personuppgifter.

Slutsatser

Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- verka för att arbetet med identifierandet av biträden och tecknandet av biträdesavtal fullföljs
- klargöra vem som ska teckna biträdesavtal och fastslå det i lämpliga styrdokument
- säkerställa att biträdesavtal tecknas samtidigt som huvudavtal tecknas
- öka kompetensen kring biträdesavtalstecknandet

4.6. Det saknas rutin för hur fånga upp revidering/uppstart av nya personuppgiftsbehandlingar

Nämnderna och styrelserna svarar att det finns ingen fastställd rutin för hur få information om när uppdateringar i pågående behandlingar gjorts alternativt hur få information om nya behandlingar som planeras.

Frågan om hur man ska fånga upp förändrade alt nya personuppgiftsbehandlingar kan få en lösning om man inför en kommungemensam behovs- och upphandlingsprocess för IT-lösningar/system. Den bör innehålla beskrivning över vart verksamheterna ska vända sig med uppkomna behov av nya eller förändrade lösningar för informationshanteringen, hur ett behov av ny IT-lösning/system ska hanteras och lämpligen som ett projekt, vilket förarbete en verksamhet själva måste göra osv. Det bör utses projektledare och övriga projektroller. Exempel på uppgifter för projektgruppen kan vara att kartlägga vilka arbetsprocesser en ny IT-tjänst ska stödja och vilken information som kommer att hanteras i dessa processer, undersöka om det uppstår nya personuppgifts-/informations-behandlingar, få en bild över vilka som kommer arbeta i nya systemet, upprätta en krav-specifikation, gå ut i upphandling, hur bedöma inkomna anbud, hur ska leveransmottagandet ske, hur arbeta med leveransgodkännandet och implementeringen och tidigt utse förvaltningsansvariga för systemet osv.

Hylte kommun har ett bra utkast klart, ”Process för införande av nya system”. Det beskriver gången från det att ett behov av ett nytt IT-system/tjänst har identifierats ute på en verksamhet och hur processen sedan ser ut i olika steg från behovsanalys och godkännande av ledning till upphandling, införande och drift. Som en delprocess finns den antagna ”Upphandlingsprocessen” med tillhörande rutiner och avtal.

I de av Hylte framarbetade förslagen till processer bör det tryckas mer på vikten av att verksamheterna ska ges stort utrymme i processen fram till att kravspecifikation och upphandling sker. Det är ju verksamheterna som bäst vet sina behov av nya arbetsverktyg och som även har bäst kännedom om vilken typ av information som genereras i verksamhetens arbetsprocesser. Det saknas även några nyckelroller som bör vara med, i den av Hylte framtagna modellen. Se mer om detta i avsnittet om nya behov och upphandling.

Slutsatser

Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- verka för att nuvarande utkast till ”Process för införande av nya system” revideras och färdigställs och därefter beslutas

4.7. En process för hantering av registerutdrag saknas

En kommungemensam process med rutinbeskrivning för hur begäran av registerutdrag ska hanteras saknas. För att de registrerade ska kunna ta tillvara sina rättigheter enligt GDPR och möjligheten att begära ett registerutdrag som visar varför och hur behandling görs av deras personuppgifter, måste en rutin och process för detta vara väl inarbetad och känd i organisationen. Den PUA som får begäran måste ha en utpekad ansvarig, t ex PUS, som samordnar utdragen. Den ansvarige kan behöva ha tillgång till registerförteckningar, dokumenthanteringsplaner, systemförteckningar och information om vilka ostrukturerade informationsmängder som finns osv.

Hylte kommun skulle i sitt arbete med att ta fram rutin och process kunna dra nytta av hur bl. a Laholm och Falkenberg arbetar vad gäller registerutdrag. I t ex Falkenberg finns en e-tjänst för begäran och den nyttjas av de flesta av nämnderna och styrelserna. Man har också tagit fram diverse instruktioner som finns tillgängliga på intranätet.

Slutsatser

Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- verka för att det snarast skapas en kommungemensam process med rutiner för hur begäran om registerutdrag ska hanteras
- verka för att rutinen kommuniceras i organisationen
- verka för att begäran hanteras digitalt via en e-tjänst

4.8. En process för incidenthantering saknas

Det finns ingen kommungemensam process med rutinbeskrivning för incidenthantering implementerad. Men däremot har kommunen tagit fram en teknisk lösning, en e-tjänst, för hanteringen. Men då rutinbeskrivningar för användandet saknas så har man därför inte kört igång den. Hylte bör därför snarast ta fram rutinbeskrivningar för hur incidenter ska hanteras och rapporteras, arbeta fram mallar för utredning av incident mm och kommunicera det i organisationen. Även i detta fall kan man dra nytta av t ex både Falkenbergs och Laholms processer och rutiner. I Laholm har processen införlivats med processen för felanmälan till IT och rapporteringen sker i samma ärendehanteringssystem. Processen där ska på sikt också automatiseras ytterligare och kopplas ihop med system för diarieföring. Det är mycket klokt att man nyttjar sedan tidigare inarbetade processer, rutiner och ärendehanteringssystem.

Det är oerhört viktigt för Hylte att få på plats en tydlig och välfungerande hantering av incidenter och det för att man snabbt ska kunna agera och vidta åtgärder för att minska eventuella negativa konsekvenser för de registrerade och för verksamheterna.

Slutsatser

Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- snarast säkerställa att interna rutiner och processer för incidenthantering upprättas och att den sedan tidigare klara e-tjänsten för incidentrapportering tas i bruk

4.8. Behandling av särskilda kategorier personuppgifter sker i olika grad inom alla nämnder och styrelser

Alla nämnder och styrelser svarar inte ja på frågan om man behandlar särskilda kategorier personuppgifter (tidigare benämnda känsliga personuppgifter).

Hyltebostäder AB svarar nej, vi behandlar inga sådana uppgifter. Dataskyddsombudet kan dock se att det bör finnas behov, och misstänker att behandling faktiskt sker, av sådana uppgifter hos Hyltebostäder. Det kan tänkas att uppgifter om t ex ekonomiska och sociala förhållanden om kunder/hyresgäster som uppgift om funktionsnedsättning eller betalningsanmärkningar behandlas m m.

Genom sättet som vissa nämnder och styrelser besvarat frågan på, kan man ana att det råder en viss osäkerhet kring vad som avses med begreppen särskilda kategorier personuppgifter och vad som anses vara i övrigt integritetskänsliga uppgifter. Det verkar bitvis också råda oklarheter kring att frågan rör hela nämndens verksamhet inte bara den ”kommuncentrala administrationens” person-uppgiftsbehandlingar utan att det kanske främst rör de behandlingar som görs ute i verksamheterna som t ex ute på skolorna. Att man svarar som man gör på denna fråga kanske beror på att det råder en otydlighet och osäkerhet kring vilka uppgifter och områden som ingår i rollen PUS ansvar.

Slutsatser

Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- verka för att kunskapen kring vad som avses med begreppen särskilda kategorier personuppgifter och integritetskänsliga personuppgifter ökar
- säkerställa ifall behandling sker av särskilda kategorier personuppgifter
- säkerställa ifall behandling av i övrigt integritetskänsliga personuppgifter sker
- tydliggöra rollen PUS ansvar, se tidigare avsnitt

4.9. Nämnder och styrelser arbetar inte alls med risk- och konsekvensbedömningar

Frågan som ställdes i granskningsunderlaget var formulerad utifrån behandling av känsliga (särskilda kategorier) personuppgifter. Enligt artikel 35.4 är det dock inte bara vid behandling av den typen av personuppgifter som konsekvensbedömning ska göras. Datainspektionen har i enlighet med artikel 35.4 antagit en förteckning över när konsekvensbedömning ska göras och den

utgör ett bra stöd i den bedömningen.

Enligt artikel 35 ska den personuppgiftsansvarige göra en konsekvensbedömning avseende dataskydd innan en behandling av personuppgifter påbörjas och i de fall då en behandling av personuppgifter sannolikt leder till hög risk för de registrerades fri- och rättigheter. Exempel på när det ska göras är vid användandet av automatiskt beslutsfattande som grundar sig på en systematisk och omfattande bedömning av människors personliga aspekter s.k. profilering. Det ska även göras när man behandlar uppgifter om lagöverträdelser eller känsliga (särskilda kategorier) person-uppgifter, till exempel uppgifter om hälsa, politisk tillhörighet, etniskt ursprung och om man behandlar personuppgifter i stor omfattning eller om man systematiskt ska övervaka en allmän plats genom kameraövervakning.

Man bör kontinuerligt se över och omvärdera sina personuppgiftsbehandlingar då förhållandena för behandlingarna kan förändras. Det kan ha uppkommit nya risker eller införts nya lagar vilka kan få följder för behandlingen.

Konsekvensbedömning är ett nytt krav som kom med införandet av GDPR. Därför behövs en kompetenshöjning på området om när och hur man ska göra dessa. Önskvärt hade varit att DI tagit fram någon arbetsmetod, en mall och en bedömningsskala för risker osv. I nuläget jobbar alla kommuner och övriga organisationer var och en på sitt håll för att hitta en metod för arbetet. Dataskyddsombudet har arbetat fram ett utkast till något som benämns ”snabbkollen” vilket är en snabbanalys över om konsekvensbedömning behöver göras eller inte. Ombudet har även tagit fram ett utkast till mall samt instruktion för konsekvensbedömning.

Hylte kommun arbetar inte alls med konsekvensbedömningar på området personuppgifts-behandlingar och bör därför snarast börja med detta.

Slutsats
Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- verka för att verksamheterna snarast börjar arbeta med konsekvensbedömningar och främst i de fall behandlingar av särskilda kategorier personuppgifter görs eller ska påbörjas för att sedan även göra konsekvensbedömningar av övriga behandlingar

4.9. Verktyg för säker digital kommunikation finns delvis på plats

Avsaknad av en lösning för att kunna kommunicera digitalt på ett säkert och lagligt sätt har varit ett stort problem i väldigt många år hos kommuner och myndigheter. Vanlig e-post, utan någon kryptering eller identitetsverifiering, är inte ett säkert sätt att kommunicera känslig information och det är inte heller lagligt att skicka känsliga personuppgifter via vanlig e-post. Det var det inte heller enligt den tidigare Personuppgiftslagen, PUL, eller enligt registerlagar inom socialtjänst och sjukvård.

Många nämnder och styrelser använder det kommungemensamma verksamhetssystemet Platina för intern kommunikation. Alla medarbetare i kommunen med tillträde till admininstratörsnätet har tillgång till Platina. Dock så har inte alla medarbetare ett konto upprättat. Det råder också en stor osäkerhet ute bland medarbetarna om hur och när man ska arbeta i Platina och många av användarna är sällan-användare. Det är mycket bra att man nyttjar de lösningar som redan finns tillgängliga i organisationen för att minimera riskerna vid behandling av känslig information.

För extern kommunikation finns det i dagsläget ingen säker digital lösning. Kommunen har dock tillgång till Trusted Dialog men man saknar en användarautentiseringslösning (IdP). När sådan är på plats kan lösningen börja användas.

Slutsats

Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- verka för att en användarautentiseringslösning (IdP) snarast kommer på plats och att lösningen Trusted Dialog därefter tas i bruk
- säkerställa att de verksamheter som behöver kommunicera känslig information och sekretessbelagda uppgifter, både internt och externt, ansluter sig till lösningen för säker kommunikation
- säkerställa att, där det är lämpligt, nyttja de verksamhetssystem, t ex Platina, som finns på plats för intern kommunikation av känsliga uppgifter

4.10. Lösning för säkra utskrifter är på plats

Alla nämnder och styrelser, förutom Hyltebostäder, har ”Follow Me Print” i merparten av sina verksamheter. Med "Follow Me Print" nås full sekretess genom att inga dokument skrivs ut förrän användaren har bestämt det och är på plats vid skrivaren. Genom att logga in får användaren access till sin egen utskrifts kö och kan därifrån fritt välja vilket eller vilka dokument som ska skrivas ut. Inloggningen kan ske genom kort, kod eller tag. Inloggningen kan synkroniseras med företagets befintliga AD (Active directory).

Många kommuner har rapporterat in incidenter till Datainspektionen som består just av utskrifter med känsliga personuppgifter som skrivits ut på fel skrivare till fel person. Men denna typ av incidenter och problem har ju däremot Hylte kommun i stort sätt helt satt stopp för med hjälp av att verktyget Follow Me nyttjas inom i princip hela kommunen. Hyltebostäder är ensam om att inte använda verktyget.

Slutsats

Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- verka för att alla verksamheter och även Hyltebostäder nyttjar Follow Me Print.

4.12. Det saknas planer för ett långsiktigt arbete med personuppgifter och dataskydd

Kommunen har inga utarbetade, långsiktiga planer för arbetet med personuppgifter och dataskydd. Många nämnder menar att nu när det finns en samordnare för informationssäkerhet på plats finns möjligheterna att bedriva ett mer aktivt, långsiktigt och strukturerat arbete på området. Självklart är det så - en utpekad och dedikerad roll för kommunens informationssäkerhetsarbete är en grundläggande förutsättning för att få fart på arbetet och för att sedan kunna upprätthålla en lämplig säkerhetsnivå för kommunens informationsmängder, inklusive skyddet för de registrerades integritet.

Man nämner också att det finns behov av utbildning inom GDPR och hur man ska arbeta för att säkerställa att lagstiftningen följs. Det behövs rutiner som bör tas fram på central nivå och därefter anpassas efter specifika behov ute i verksamheterna.

I princip alla nämnder och styrelser anser alltså att det finns ett behov av en plan för arbetet med personuppgifter. I nuläget kan det vara bra att en kommungemensam plan upprättas. Fokus bör ligga på att hitta en struktur för arbetet. En tanke kan vara att arbeta utifrån ett ”årshjul” och att arbeta in dataskyddsfrågor i den ordinarie verksamhetsplanen. Det finns en vinst med att försöka nyttja redan etablerade processer och verktyg för det långsiktiga arbetet istället för att skapa nya processer som ska arbetas in i organisationen. Att få in området informationssäkerhet och dataskydd enligt GDPR i kommunens etablerade processer för planering, styrning, ledning och internkontroll, bör vara den mest framgångsrika vägen för arbetet.

Uppstart av arbetet med en plan för dataskydd sker lämpligen i det forum för PUS som ska startas upp. Planen bör innehålla områden som ska prioriteras gemensamt för alla verksamheter och resultatet från denna granskningsrapport kan lämna bidrag till planens innehåll. Större kommungemensamma frågor som uppkommer i forumet/nätverket kan behöva hanteras i projektform och kanske lyftas till kommunledningen som får ta beslut om vad som ska prioriteras.

Det är viktigt att upprätthålla medvetandet kring personuppgiftshanteringsområdet. Genom att skapa en plan med aktiviteter och diverse uppföljningar och som dessutom finns med i ordinarie årshjul, då kommer ämnet att ständigt vara närvarande och framförallt i diverse ledningsforum.

Slutsats

Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- säkerställa att arbetet med dataskydd enligt GDPR och det totala arbetet med informationssäkerhet arbetas in i kommunens redan etablerade processer för planering, ledning, styrning och kontroll

- verka för att det snarast upprättas en kommungemensam plan med prioriterade arbetsområden

4.13. En samordnad process för hur behov av nya IT-lösningar ska hanteras är inte implementerad

I Hylte kommun finns det två olika processer som tillsammans bildar en grund för hur en upphandling kan gå till; ”Process för införande av nya system” (se bilder 1a – 1d, tidigare redovisade i kap 3 ovan) beskriver gången från att ett behov av ett nytt IT-system/tjänst har identifierats ute på en verksamhet och hur processen sedan ser ut i olika steg från behovsanalys och godkännande av ledning till upphandling, införande och drift. Denna process är under utveckling och är inte ännu antagen.

Som en delprocess finns ”upphandlingsprocessen” (se bild 2, tidigare redovisad i kap 3 ovan) som är antagen med tillhörande rutiner och avtal. Upphandlingsprocessen finns beskriven på kommunens intranät så alla medarbetare har tillgång till den.

Det är mycket bra att kommunen arbetat fram dessa processer. De behöver dock revideras/ kompletteras i vissa delar och sedan snarast beslutas och implementeras.

En IT-lösning/system är inget självändamål i sig. IT ska utgöra ett stöd, ett verktyg, för verksamheternas arbetsprocesser. I system och IT-lösningar genereras mängder av information genom de arbetsprocesser som utförs däri. Fokus har sen länge, generellt sett, legat på tekniken och dess utveckling, inte på de processer och den information som tekniken ska stödja. Digitalisering består till 90 % utav förändrade arbetssätt. Alltför många ser ett nytt system som målet för sina projekt men i själva verket är systemet bara ett medel för att uppnå helt andra effekter. Mot bakgrund av detta finns anledning att tänka om på flera punkter när det gäller digitalisering och informationshantering.

En kommungemensam process bör bygga på tanken ”en väg in” för kommunens samtliga uppkomna behov av nya IT-lösningar. Det betyder att inga upphandlingar av lösningar får ske av verksamheterna själva och inte heller av IT-enheten självt. Kravställning och upphandling sker enligt processen vilken ska bygga på samarbete mellan ett antal berörda och givna enheter och roller. Behovet ska ”anmälas” till en huvudansvarig avdelning/enhet. Det är viktigt att denna enhet har ett kommunövergripande och strategiskt perspektiv i sitt arbete. Lämpligen en enhet på den centrala kommunstyrelseförvaltningen. Arbetet med behovsanalys, kravställning och upphandling ska alltid utgå från verksamheternas behov. Verksamheter ska inte kunna tilldelas en IT-lösning som de inte varit med och kravställt. Dessutom är respektive nämnd informationsägare och personuppgiftsansvarig enligt Dataskyddsförordningen för den information som hanteras i IT-lösningen.

En kommunövergripande, samordnad och tydlig process för nya behov av IT-tjänster kan överskådligt beskrivas i följande tre huvudmoment (utgår från MSBs förslag på inköpsprocess);

FÖRBEREDA	UPPHANDLA	REALISERA
• **Genomföra förstudie**	• **Identifiera behov och krav** • **Utvärdera och tilldela**	• **Kontrollera leverans** • **Förvalta** • **Avsluta**
• Identifiera behov	• Besluta att behovet ska realiseras med upphandling	• Säkerställa att leveransen uppfyller ställda krav
• Identifiera information	• Identifiera ansvar	• Godkänna leverans
• Genomföra initial klass-ning av informationen	• Genomföra fördjupad informationsklassning	• Följa upp att säkerhets-kraven uppfylls över tid
• Bedöma relevansen av krisberedskap och sam-hällsviktig verksamhet	• Genomföra fördjupad riskbedömning	• Identifiera behov av förändringar
• Identifiera interna krav och behov	• Identifiera säkerhetskrav	• Förbereda avslut av leverantörsrelationen
• Identifiera externa krav och behov	• Definiera utvärderingsmodell för säkerhetskrav	• Ta hem informationen
• Genomföra initial riskbedömning	• Färdigställa upphandlingsunderlag	• Säkerställa att ingen information finns kvar hos leverantören
• Besluta om hur behovet ska realiseras	• Godkänna upphandlingsunderlag	
	• Utvärdera leverantörer	
	• Utvärdera kravuppfyllnad	
	• Fatta tilldelningsbeslut	
	• Skriva avtal	

Källa: MSB utifrån Upphandlingsmyndighetens inköpsprocess

I förstudien är det viktigt att utreda vilka verksamhetsprocesser och medarbetare som tjänsten ska stödja. Där bör också klargöras vilken kompatibilitet med övrig IT-infrastruktur som krävs och önskas. Vilken information som kommer att hanteras i IT-lösningen och vilken information som den externa aktören eventuellt kan komma att få tillgång till under avtalstiden, det är två mycket viktiga delar att skaffa sig kunskap om.

En initial klassning av informationen utifrån krav på konfidentialitet, riktighet och tillgänglighet ska också göras i denna fas.

Identifiera interna och externa krav som finns i diverse interna policyer, avsiktsförklaringar, anvisningar, riktlinjer, strategier eller motsvarande. Externa krav kan vara rättsliga krav eller övriga externa behov som finns för den tjänst som ska upphandlas. Till exempel EU-förordningar, EU direktiv och internationella konventioner, Svenska lagar och förordningar.

Roller som bör delta i projektet kan vara representanter för de arbetsprocesser IT-lösningen ska stödja, centralt digitaliseringsansvariga, verksamhetsutvecklare, systemförvaltare, kommun-arkivarie/specialist informationshantering, It-tekniker, informationssäkerhetssamordnare, teknisk informationssäkerhetssamordnare, dataskyddsombud, personuppgiftssamordnare, IT-arkitekt och upphandlare. En projektledare ska tillsättas som samordnar arbetet och utformar projektdokument, kallar till avstämningsmöten, bevakar deadlines m m. Det kan också vara lämpligt att redan i detta läge knyta en kommunikatör till projektet.

Förstudien ska helt enkelt identifiera vilka grundförutsättningar som föreligger för att sedan fatta beslut om det är aktuellt med upphandling eller om behovet ska lösas på ett annat sätt.

I fasen Upphandla presenteras förstudien. Beslut tas om att behovet ska realiseras med upphandling (eller genom annan lösning). I detta moment görs, om behov finns, en fördjupning av delarna i förstudien. Ansvar måste identifieras, upphandlingsunderlag färdigställas och godkännas. Utvärdering och kravuppfylland av leverantörer görs. Det är viktigt att inkomna bud utvärderas mot ställda säkerhetskrav. Tilldelningsbeslut fattas och avtal (inklusive eventuellt personuppgifts-biträdesavtal) skrivs. I detta moment deltar flertalet av rollerna som angetts ovan i förberedelse-fasen.

I Realisera-fasen säkerställs att leveransen uppfyller ställda krav och därefter sker ett leverans-godkännande. Över tid ska man följa upp att säkerhetskraven uppfylls, om behov finns av förändringar, förbereda avslut av den ev. tidigare leverantörsrelationen och ta hem all information. I detta moment deltar ett färre antal av rollerna som angetts ovan.

Att arbeta utifrån en tydlig process får många positiva effekter för kommunen;

- man får kontroll över vilka system och IT-tjänster som nyttjas och var kommunens informationsmängder finns
- samordningsvinster – allt ifrån ekonomiska vinster till en mer effektiv och praktisk hantering av IT-upphandlingar
- tidsbesparande - man har en känd och fastställd modell för hur arbetet ska bedrivas när nytt behov av IT-lösning uppstår
- kvaliteten på upphandlingsunderlag blir högre då det gjorts en bred analys av verksamhetens behov och med deltagande av olika kompetenser/roller, vilket minskar risken för att man köper in en IT-lösning som inte stödjer arbets-processerna, som inte fungerar ihop med övrig IT-infrastruktur och som inte är säker och inte heller är juridiskt hållbar.

Slutsats

Berörda personuppgiftsansvariga nämnder, styrelser samt chefer och ledningspersoner bör;

- verka för att Hylte kommuns utkast till ”Process för införande av nya system” färdigställs samt kompletteras så att den får ett ökat fokus på verksamheternas behov och att ett kommunövergripande samarbete genomsyrar modellen samt att den därefter beslutas
- fastställa roller som i princip alltid behöver vara delaktiga i arbetet med hantering av nytt behov av IT-lösning och i fortsatta process för upphandling.

Avslutning

Rapporten lämnas över 2020-02-28 till registraturen vid Hylte kommun för vidare expediering till samtliga personuppgiftsansvariga, d.v.s. nämnder och styrelser, samt till högsta förvaltningsledningen.

Jessica Karlsson
Dataskyddsombud för Falkenberg, Laholm och Hylte

Bilaga 1.
Definitioner och förklaringar av begrepp

Nämnder och styrelser: de politiskt ledande församlingarna i kommunerna och bolagen, som var och en är personuppgiftsansvariga, PUA, för sin egen och för sin förvaltning och dess verksamheters personuppgiftshantering.

Förvaltningar och verksamheter: tjänstemannaorganisationen under respektive nämnd och styrelse och de olika delarna inom en förvaltning, som utför det praktiska arbetet utifrån tagna politiska beslut samt aktuell lagstiftning. I rapporten används oftast begreppet nämnd och då inkluderas även dess förvaltning.

Personuppgift: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Beroende på personuppgifternas skyddsvärde så talar man om **följande klassificeringar/kategorier;**

Harmlösa personuppgifter; t ex namn, efternamn, telefonnummer, adress, email, etc.

Extra skyddsvärda personuppgifter*;* personnummer, personuppgifter som är hänförliga till individer under 18 år, uppgifter om lagöverträdelser, värderande uppgifter som till exempel uppgifter från utvecklingssamtal, om resultat från personlighetstester, information som rör någons privata sfär, uppgifter om sociala förhållanden (kan vara uppgifter som faller under **sekretess**).

Särskilda kategorier personuppgifter GDPR artikel 9,10 (*känsliga personuppgifter*); personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning (kan vara uppgifter som faller under **sekretess**).

Behandling: varje åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Personuppgiftsansvarig, PUA: en fysisk men oftast en juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms

av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Personuppgiftsbiträde, PUB: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning och som finns utanför den egna organisationen.

Personuppgiftsbiträdesavtal: avtal i vilket den personuppgiftsansvarige, förtydligar och ger instruktioner till biträdet om hur, när och vem som får behandla PUAs personuppgifter.

Dataskyddsombud, DSO: den som behandlar personuppgifter måste oftast utse ett dataskyddsombud. Ombudets roll är att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.

Personuppgiftssamordnare, PUS: har ett övergripande ansvar i verksamheterna för att register förs över personuppgiftsbehandlingar, arbeta med att säkerställa att kunskapsnivån är tillräckligt hög i organisationen,

Registerförtecknare, RF: är ansvarig för att registrera, och uppdatera personuppgifts-behandlingar, har god kunskap om behandlingarna och god kunskap om verksamheten i vilken behandlingen görs.

Registerförteckning: både personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att föra ett register eller en förteckning över behandlingar av personuppgifter. Dessa register ska upprättas skriftligen, vara tillgängliga i elektronisk format och hållas uppdaterade. På begäran ska registret göras tillgängligt för Datainspektionen. Vad som ska finnas med i förteckningen beskrivs i artikel 30 i dataskyddsförordningen. Registret ska innehålla bl. a följande uppgifter:

- kontaktuppgifter för den personuppgiftsansvarige samt dataskyddsombudet.
- ändamålen med behandlingen.
- en beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.
- mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.
- i tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

Registerutdrag: den registrerade har rätt att av den personuppgiftsansvarige få bekräftelse på om personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige i en lättillgänglig, skriftlig form och med ett tydligt och enkelt språk

Informationssäkerhet: Information är medlet för att förmedla kunskap. Vi kan kommunicera information, vi kan lagra den, vi kan förädla den och vi kan styra processer med den – vi behöver den för det mesta vi gör helt enkelt.

En del av vår information är värdefull, både för organisationer och för den enskilda människan. Allt från forskningsresultat och fotografier till fastighetsförteckningar och saldot på vårt bankkonto. Ibland till och med livsviktig såsom informationen i patientjournaler eller styrsystemen i kärnkraftverk. Är den informationen förlorad eller felaktig kan det få katastrofala följder. Därför måste vi skydda vår information så:

- att den alltid finns när vi behöver den (tillgänglighet)
- att vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- att endast behöriga personer får ta del av den (konfidentialitet)

Skyddet behöver givetvis anpassas efter behovet så att det är tillräckligt bra och inte för svagt eller alltför krångligt och dyrt. De konsekvenser som kan inträffa med bristande skydd är för höga för att försummas.

Arbetet med informationssäkerhet omfattar att införa och förvalta **administrativa regelverk** så som policys, riktlinjer och lagefterlevnad och ett **tekniskt skydd** med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd. Det handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge organisationens information det skydd den behöver.

Personuppgiftsincident: en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.