Vägledning
Datum 2020-12-21
Diarienummer: RS 2020-04196

Västra Götalandsregionen
Koncernkontoret
Handläggare: Lina Kolsmyr,
Charlotta Tengbert
E-post: lina.kolsmyr@vgregion.se,
charlotta.tengbert@vgregion.se

Elektroniska underskrifter

Bakgrund

I samhället i stort pågår en digitalisering av information och tjänster. Inom Västra Götalandsregionen (VGR) har man de senaste åren vidtagit åtgärder för att digitalisera informationshanteringen, bland annat genom att införa ärendehanteringssystemet Public 360 och samarbetsytor med e-arkivfunktionalitet. Övergången till aktivitetsbaserade kontor innebär också behov av ökad digitalisering och minskad pappershantering.
En del handlingstyper hanteras i analog form på grund av behov av underskrift, till exempel protokoll och avtal som ska undertecknas av olika parter. Både inom och utom VGR framkommer behov av att kunna hantera underskrifter elektroniskt.
Uttrycket *elektronisk underskrift* är den formella benämningen i svensk lag och EU-rätt till motsvarigheten av ”egenhändig underskrift” i digital miljö. Det finns många olika krav som behöver vara uppfyllda för att den elektroniska underskriften ska vara accepterad, giltig och kunna bevaras på samma sätt som analoga underskrifter.

Denna vägledning är tänkt att vara till stöd och hjälp då man överväger att införa nya systemlösningar för elektroniska underskrifter i VGR. En arbetsgrupp bestående av sakkunniga inom olika berörda områden har deltagit i arbetet; Lina Kolsmyr (juridik), Charlotta Tengbert (arkiv- och informationshantering), Göran Hallsten (upphandling), Fredrika Holm (informationssäkerhet), Susanne Lindqvist, Johan Wretborn, Sarah Live Ericsson (objekt Diarium och dokumenthantering), Fredrik Rasmusson (e-legitimering), Tommy Radniecki (IT-säkerhet) samt Jesper Bergman (systemadministratör Västfastigheter). Vägledningen publicerades 2020-09-02 som första version och på nytt med uppdateringar 2020-12-21.

Behov av elektronisk underskrift

Inom VGR har identifierats ett behov av att underteckna framför allt protokoll från politiska sammanträden, interna överenskommelser och avtal med externa parter elektroniskt. Därutöver finns en mängd ytterligare handlingstyper som skulle kunna vara aktuella för elektroniska underskrifter.

Det finns många arbetsuppgifter där det behövs någon form av godkännande eller attest. Det innebär inte att det krävs en egenhändig namnunderskrift. Det kan istället lösas genom behörighetshantering och inloggning i ett system.

Regelverk om krav på e-underskrifter

Definition

En *elektronisk underskrift* definieras i eIDAS-förordningen som uppgifter i elektronisk form som är fogade till eller logiskt knutna till andra uppgifter i elektronisk form och som används av undertecknaren för att skriva under.

En elektronisk underskrift syns inte, utan består av elektronisk information som bara kan tolkas av en dator. Det finns ingen grafisk symbol eller liknande som visar att ett elektroniskt dokument signerats med elektronisk underskrift.

eIDAS-förordningen

Den 1 juli 2016 började EU:s förordning 910/2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden (eIDAS-förordningen) att tillämpas i Sverige. eIDAS-förordningen är för närvarande föremål för en översyn.

Syftet med förordningen är att öka förtroendet för elektroniska transaktioner på den inre marknaden genom att tillhandahålla en gemensam grund för ett säkert elektroniskt samspel mellan privatpersoner, företag och den offentliga förvaltningen. Avsikten är därigenom att öka effektiviteten hos offentliga och privata digitala tjänster, affärsverksamhet och e-handel i unionen.

Exempel på betrodda tjänster som omfattas av eIDAS-förordningen är elektroniska underskrifter och stämplar, validering och bevarande av elektroniska underskrifter och stämplar, tjänster för rekommenderad elektronisk leverans och utfärdande av certifikat för autentisering av webbplatser.

eIDAS-förordningen innebär att tillhandahållare av betrodda tjänster ska vidta lämpliga tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten hos de betrodda tjänster som de tillhandahåller.

eIDAS-förordningen reglerar bland annat offentliga organs skyldighet att ta emot elektroniskt underskrivna handlingar och innebär att det finns ett allmänt krav på att en underskrift inte får avvisas enbart baserad på det faktum att den är elektronisk. Undantag gäller om det finns särskilda formkrav i svensk författning, vilket beskrivs närmare nedan.

Avancerad och kvalificerad e-underskrift

Det finns tre ”nivåer” av e-underskrifter; elektronisk underskrift, avancerad elektronisk underskrift och kvalificerad elektronisk underskrift, där eIDAS-förordningen ställer olika krav.

För att skapa den enklaste formen av *elektronisk underskrift* enligt definitionen ovan krävs inte någon verifiering av användarens identitet, utan det är fråga om uppgifter i elektronisk form som används för att kontrollera att innehållet kommer från den som har undertecknat handlingen.

En *avancerad elektronisk underskrift* uppfyller därutöver följande krav. Den är uteslutande knuten till en undertecknare som kan identifieras genom den. Den avancerade elektroniska underskriften är skapad på ett sådant sätt att undertecknaren har kontroll över den. Ändringar i den avancerade elektroniska underskriften kan upptäckas.

En *kvalificerad elektronisk underskrift* är en avancerad elektronisk underskrift som skapas med hjälp av en kvalificerad anordning för underskriftsframställning och som är baserad på ett kvalificerat certifikat för elektroniska underskrifter.

En stor del av kraven inom eIDAS-förordningens del om betrodda tjänster är kopplade till kvalificerade e-underskrifter. Dessa gäller i alla EU-länder i alla situationer där det saknas formkrav i nationell författning.

E-underskriftens förhållande till e-legitimering

eIDAS-förordningen är uppdelad i två delar. En del handlar om elektronisk identifiering och en del handlar om betrodda tjänster. E-legitimering är ett medel för en person att identifiera sig elektroniskt.

För e-legitimering finns olika tillitsnivåer som innebär olika grad av säkerhet i teknik och identifiering. Det är viktigt att skilja på e-legitimeringens tillitsnivå och nivån på e-underskriften. Lagstadgade e-underskrifter kan som nämnts ovan vara avancerade eller kvalificerade. Tillitsnivån beskriver hur säkra rutinerna och tekniken bakom legitimeringen av användaren är.

Det finns fyra tillitsnivåer, grad av säkerhet, för e-legitimering enligt internationell standard som *Myndigheten för digital förvaltning, DIGG*, tillämpar, bland annat i samband med kvalitetsmärket Svensk e-legitimation. Ju högre tillitsnivå en e-legitimation har, desto säkrare är e-legitimeringen.

De utländska e-legitimationerna inom e-IDAS har tillitsnivåerna "låg", "väsentlig" och "hög". Dessa tillitsnivåer skiljer sig från de svenska. Tillitsnivå "låg" ligger betydligt lägre än den svenska tillitsnivå 2. Tillitsnivå "väsentlig" motsvarar nivå 3 enligt kvalitetsmärket Svensk e-legitimation. Tillitsnivå "hög" inom e-IDAS är nästan att likställa med Sveriges nivå 4 med undantag för att ”hög” inte kräver personliga besök vid förnyelse av e-legitimationen, vilket tillitsnivå 4 gör.

För att skapa en kvalificerad e- underskrift behöver e- legitimeringen som kopplas till e- underskriften ligga på minst tillitsnivå 3 (e-IDAS ”väsentlig”). För att skapa en avancerad e-underskrift behöver e-legitimeringen som kopplas till e-underskriften vara på tillitsnivå 2 (e-IDAS ”låg”) eller högre.

Hinder mot e-underskrift

eIDAS-förordningen påverkar inte svensk nationell rätt som avser ingående av avtal och formkrav för avtals giltighet. Med *formkrav* menas att en handling för att ha en viss rättsverkan ska ha viss form eller visst innehåll eller ska tillkomma eller annars hanteras på ett visst sätt. Om en handling enligt en formföreskrift i lag ska vara försedd med underskrift kan detta krav inte uppfyllas med elektroniska

rutiner. Sådana formföreskrifter är inte särskilt vanliga. E-underskrifter kan därför normalt användas. Exempel på formkrav som hindrar användning av e-underskrifter är bestämmelsen i 4 kap 1 § jordabalken om att köp av fast egendom sker genom upprättande av köpehandling som skrivs under av säljaren och köparen och bestämmelsen i 10 kap 1 § ärvdabalken om att testamente ska upprättas skriftligen med två vittnen.

I VGR:s verksamheter har vi hittills endast identifierat fastighetsöverlåtelser som ett sådant område där det finns formkrav som utgör hinder mot e-underskrifter.

Krävs underskrift?

En annan fråga är om handlingar överhuvudtaget behöver undertecknas.
Krav på att en *myndighets beslut* ska vara underskrivna gäller endast om det föreskrivs i lag, förordning eller myndighetsföreskrifter. Sådana krav är ovanliga. De skyddsbehov som ligger till grund för att en myndighets beslut upprättas skriftligt kan normalt tillgodoses i elektronisk miljö utan underskrift (se eSams vägledning sid 28).

När det gäller *protokoll från politiska sammanträden* inom VGR föreskriver 5 kap 69 § kommunlagen att ett protokoll ska justeras senast fjorton dagar efter sammanträdet på det sätt som fullmäktige har bestämt. Enligt en dom från kammarrätten i Göteborg den 24 september 2014 (mål nr 3459-14) finns inte hinder mot att justera sammanträdesprotokoll med elektronisk signatur.

Vad avser *ansökningshandlingar* och liknande skrifter till en myndighet finns krav på att sådana ska vara underskrivna på papper eller elektroniskt endast om sådan form krävs enligt lag, förordning eller myndighetsföreskrifter (se eSams vägledning sid 29 f).

Beträffande *upphandlingar* som genomförs inom VGR kan konstateras att en upphandlande myndighet enligt 12 kap 7 § lagen om offentlig upphandling får kräva att elektroniska anbudshandlingar och anbud ska vara försedda med en sådan avancerad elektronisk underskrift som avses i e-IDAS-förordningen.

Avtal kräver inte för sin giltighet att det undertecknats. Undertecknande sker dock vanligtvis och bör så ske av flera olika skäl.

Underskriftens funktion

När det inte finns någon formföreskrift som kräver att en handling skrivs under får myndigheten göra en bedömning utifrån vilken kategori av handling det är fråga om och vilka av underskriftens funktioner som behöver ersättas av annat tekniskt eller administrativt skydd (se eSams vägledning sid 30).

Handlingar skrivs under elektroniskt för att ge *skydd mot förfalskning och förnekande* på motsvarande sätt som när handlingar undertecknas på papper. Underskriftens funktion är främst *säkerhetsrelaterad*, såsom att ge underlag för *äkthetsprövning* (kontroll av vem som skrivit under och att handlingens innehåll inte har ändrats, *bevissäkring* (ett skriftligt bevis skapas), och *originalkvalitet* (det

blir möjligt att skilja handlingar som kan kontrolleras på ett tillförlitligt sätt från oskyddade handlingar).

När handlingens äkthet inte måste skyddas genom underskrift kan andra skyddsfunktioner som underskrifter erbjuder föra med sig krav på undertecknande, såsom *avslutningsfunktionen* (att innehållet är fullständigt och förenligt med utställarens avsikt), och *varningsfunktionen* (att tänka sig för och förstå åtgärdens innebörd), (se eSams vägledning sid 22 f).

Är det huvudsakliga syftet, bakom att en viss kategori av handlingar skrivs under, säkerhetsrelaterad kan underskrifter behövas antingen på papper eller elektroniskt. En myndighet som tar emot handlingar elektroniskt bör genom en riskanalys klarlägga vilka av underskriftens funktioner som är centrala för berörda förfaranden och i vilken mån tekniskt, administrativt och rättsligt skydd kan ges med andra metoder (se eSams vägledning sid 30).

Underskriftens säkerhetsnivå

Svensk lagstiftning ställer inte krav på användning av kvalificerade elektroniska underskrifter, utan förekommande krav tar sikte på avancerade elektroniska underskrifter.

Det finns inga krav på medlemsstaterna att använda sig av kvalificerade elektroniska underskrifter. Sådana krav kan dock komma att ställas genom olika former av gränsöverskridande tjänster eller samarbeten. De svenska direkta och indirekta underskrifterna anses generellt sett uppfylla kraven för avancerade elektroniska underskrifter.

Kvalificerade elektroniska underskrifter ska enligt eIDAS-förordningen ha samma rättsliga verkan som en handskriven underskrift. Detta hindrar dock inte att svensk lagstiftning ger även andra former av elektroniska underskrifter samma rättsliga verkan som en handskriven underskrift (se eSams vägledning sid 60 f).

Pågående statlig utredning om betrodda tjänster

Enligt kommittédirektiv (dir 2020:27) beslutade av regeringen den 12 mars 2020 ska en särskild utredare (Henrik Ardhede) utreda förutsättningarna för ökad och standardiserad användning av betrodda tjänster i den offentliga förvaltningen.

Syftet med utredningen är att höja säkerheten och stärka tilliten när betrodda tjänster används. Uppdraget ska redovisas senast den 30 december 2020.
I utredarens uppdrag ingår att kartlägga och analysera den offentliga förvaltningens behov av åtgärder för ökad och standardiserad användning av betrodda tjänster och lämna förslag på sådana åtgärder, särskilt när det gäller att

- tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen
- kunna validera och bevara elektroniska underskrifter, och
- kunna använda e-legitimation i tjänsten.

Andra myndigheters och organisationers uppdrag och information

Myndigheten för digital förvaltning, DIGG, ansvarar för Sveriges åtaganden inom e-legitimering. På myndighetens hemsida finns information om e-underskrifter.

DIGG rekommenderar att offentlig sektor som förstahandsval, erbjuder användarna e-tjänster med e-underskriftsmöjlighet mot bakgrund av att eIDAS-förordningen innehåller krav på offentliga organ att ta emot e-underskrifter i en rad olika format. Det kommer troligen även att minska volymen elektroniskt underskrivna dokument av olika slag, som användaren sänder in, och hanteringen blir normalt sett enklare.

Vid införande av en fristående underskriftstjänst som följer DIGG:s riktlinjer fungerar e-underskrifter även med utländska e-legitimationer. En sådan e- underskrift är i dagsläget att betrakta som en avancerad e-underskrift enligt eIDAS.

Post och Telestyrelsen, PTS, har tillsynsansvar för e-underskrifttjänster och andra betrodda tjänster enligt eIDAS-förordningen och har information om betrodda tjänster på myndighetens hemsida.

eSam är ett medlemsdrivet program för samverkan mellan 27 myndigheter och SKR som vill ta tillvara digitaliseringens möjligheter. eSam ger ut stöddokument för personer som arbetar med digital utveckling i samverkan inom offentlig sektor och har tagit fram en juridisk vägledning för införande av e-legitimering och e-underskrifter.

Inera AB ägs av Sveriges Kommuner och Regioner, SKR, genom SKR Företag, samt regioner och kommuner. Ineras uppdrag är dels att utveckla och förvalta gemensamma, kvalitetssäkrade tjänster, dels att koordinera den digitala utvecklingen och tillhandahålla kompetens och material som stödjer regioners och kommuners verksamhetsutveckling genom digitalisering. Inera har tagit fram referensarkitektur för elektronisk underskrift och stämpel och har även för ägarnas räkning upphandlat sådana tjänster.

Riksarkivet är en statlig förvaltningsmyndighet under Kulturdepartementet och har ett särskilt ansvar för den statliga arkivverksamheten och arkivvården i Sverige. Riksarkivets uppdrag regleras i arkivlagen, arkivförordningen och i Förordning med instruktion för Riksarkivet samt i årliga regleringsbrev med specifika uppdrag. Riksarkivet är också normgivande för kommunala och regionala myndigheter i vissa fall. Riksarkivet har utrett frågan om bevarande av elektroniska underskrifter, https://riksarkivet.se/elektroniskasignaturer

Slutsatser om juridiska krav

Inför köp av lösning för elektronisk underskrift behöver VGR ta ställning till vilka handlingar som den elektroniska underskriften ska användas för. Ett första steg är att bedöma om underskrift behövs på de aktuella handlingarna eller om skälen för underskrift istället kan tillgodoses på andra sätt för att ge handlingen ett tillräckligt tekniskt eller administrativt skydd.

Om skälen för att en handling skrivs under utgörs av att kunna säkerställa handlingens äkthet och säkra dess värde som bevis talar det för att en underskrift behövs. För avtal som VGR ingår med externa parter bedöms inte underskriftens funktion kunna ersättas av annat skydd, utan dessa bör undertecknas. Undertecknandet kan ske elektroniskt om det inte finns ett särskilt formkrav i lag såsom vid fastighetsöverlåtelser.

Beroende på vilken funktion underskriften ska fylla behöver också ställningstagande ske till vilken nivå som den elektroniska underskriften ska uppnå. Svensk lagstiftning ställer i dagsläget inte krav på användning av kvalificerade elektroniska underskrifter. Det ska dock noteras att den pågående statliga utredningen om betrodda tjänster ska lämna förslag på åtgärder för att tydliggöra när avancerade respektive kvalificerade elektroniska underskrifter bör användas i den offentliga förvaltningen.

En avancerad elektronisk underskrift innebär att den som undertecknat handlingen kan identifieras genom underskriften. E-legitimeringen som kopplas till e-underskriften behöver för att skapa en sådan avancerad elektronisk underskrift vara minst på tillitsnivå 2 (eIDAS ”låg”).

För avtal och andra handlingar där äktheten behöver kunna säkerställas bedöms inte tillräckligt med en lägre nivå av elektronisk underskrift där användarens identitet inte kan verifieras, utan i dessa fall bedöms en avancerad elektronisk underskrift behövas.

För interna handlingar som upprättas inom VGR kan dock tänkas att en lägre nivå av elektronisk underskrift är tillräcklig, beroende på vilket syfte underskriften ska fylla.

Bevarande och arkivering

Arkivlag och styrande dokument

Arkivlagen (1990:782) ställer krav på att myndigheternas arkiv ska bevaras, hållas ordnade och vårdas så att de tillgodoser rätten att ta del av allmänna handlingar, behovet av information för rättskipningen och förvaltningen, samt forskningens behov. Regionfullmäktige har fattat beslut om Föreskrifter och riktlinjer om arkiv- och informationshantering och arkivmyndigheten Arkivnämnden i Göteborgs stad och Västra Götalandsregionen har tagit fram anvisningar om tillämpningen av dessa föreskrifter och riktlinjer. Där framgår bland annat att alla myndigheter inom VGR ska fatta beslut om sin dokumenthanteringsplan och av den ska det framgå hur länge olika handlingstyper ska bevaras. Protokoll och avtal är exempel på handlingar som ska bevaras för alltid.

Arkivbeständighet

Allmänna handlingar ska framställas så att de kan bevaras under hela sin livstid. Det är därför viktigt att använda sig av arkivbeständiga material och metoder. Arkivlagen ställer krav på att myndigheten skall skydda arkivet, de allmänna handlingarna, mot förstörelse, skada, tillgrepp och obehörig åtkomst. Det innebär i detta fall att handlingarna ska framställas i arkivbeständiga format och att den elektroniska underskriften också ska kunna

bevaras. För elektroniska kontorsdokument gäller idag arkivbeständiga format inom PDF/A. Det är viktigt att välja rätt arkivbeständigt format som den tekniska systemlösningen stödjer, så att inte det ursprungliga skicket ändras vid konvertering. Det bör framgå av själva handlingen *vem* som har undertecknat (namnförtydligande) och *när* (datum) så att det kan läsas i klartext.

Bevarandet av elektroniska underskrifter innebär att den elektroniskt underskrivna allmänna handlingen (informationsmängden) såväl som underskriften ska bevaras. Alla komponenter som utgör den elektroniskt underskrivna allmänna handlingen ska vara i ursprungligt skick.

Den tekniska systemlösning som den elektroniskt underskrivna handlingen för stunden ligger i ska kunna säkerställa handlingarnas integritet och autenticitet. Att ett system beräknar checksummor (kontrollsummor) för handlingar är en metod för att upptäcka eventuell förstörelse eller tillgrepp. Därför ställer arkivmyndigheten krav på att den tekniska systemlösningen säkerställer att checksumma, och metod som checksumman beräknats med, lagras som separat metadata. Det räcker inte att checksumma finns för det enskilda dokumentet, utan det är systemet där handlingen slutförvaras efter underskrift, registrering och arkivering som behöver ha funktion för checksumma. I praktiken kräver det att funktionaliteten för elektronisk underskrift är integrerad med den tekniska systemlösningen för slutförvaring så att ingen förändring kan ske från att underskriften har tillkommit fram till att handlingen låses in. Varje gång den elektroniskt underskrivna allmänna handlingen överförs till ny plats för lagring under sin bevarandetid, ska alla komponenter fortsätta vara i ursprungligt skick. Detta gäller även metadata. Det bör också nämnas att handlingen behöver vara i just det arkivbeständiga format som den tekniska systemlösningen kan hantera så att den inte förstörs vid eventuell konvertering.

Bevarande av giltighet

En skillnad måste göras mellan att bevara en underskrift som den var och att bevara att underskriften var eller är giltig. Bevarandet av en elektronisk underskrift i ursprungligt skick innebär inte att signaturens giltighet har bevarats, det vill säga att underskriften var giltig när den gjordes eller att den fortfarande är giltig.

Valideringen av en elektronisk underskrift, det vill säga kontrollen att underskriften är giltig, är beroende av en ”yttre legitimitet”. En liknelse är att jämföra med en handskriven underskrift som kan kontrolleras med någon typ av identitetshandling såsom ett ID-kort eller pass vid tillfället för undertecknande.

En elektronisk underskrift är bevarad så länge dess autenticitet inte kan ifrågasättas eller äventyras. Det bör vara tillräckligt att man kan visa att en underskrift var giltig en gång i tiden vid dess framställande innan nycklar och certifikat senare återkallades eller upphörde att gälla. Riksarkivet har i sin rapport Framställning och bevarande av elektroniska signaturer 2014-2015 resonerat kring två sätt att långsiktigt bevisa giltigheten i en elektronisk underskrift från när den utfärdades. Ett sätt är en rekursiv tidsstämpel som man förnyar med jämna mellanrum och där den obrutna kedjan av valideringar visar att underskriften var korrekt när den gjordes. Ett annat sätt är systemberoende, dvs att det system för bevarande som handlingen med den elektroniska underskriften förvaras i upprätthåller att handlingen med alla dess komponenter bevaras i ursprungligt skick, att tekniska och/eller systematiska åtgärder tillsammans skapar ett system som kan validera ett dataobjekt genom att säkerställa att dataobjektet inte har förändrats. Med detta menas

åtgärder som t ex. behörighetskontroll, loggning, arbetsrutiner och checksumma. Man ska veta att den elektroniska underskriften var korrekt när den lades i systemet, sedan upprätthåller systemet autenticiteten och integriteten av dokumentet.

Slutsatser om bevarande

För att bevara en elektronisk underskrift krävs att

- Handlingen ska framställas i rätt arkivbeständigt format som också fungerar i den tekniska systemlösningen där handlingen ska slutförvaras
- Handlingen och den elektroniska underskriften ska bevaras i ursprungligt skick från när underskriften gjordes.
- Checksumma (kontrollsumma) och metod som checksumman beräknats med ska lagras som separat metadata i det system där handlingen ska slutförvaras.
- Handlingen med den elektroniska underskriften ska förvaras i ett system som genom rutiner och tekniska åtgärder garanterar att handlingen är helt intakt under handlingens hela bevarandetid.
-

Om framställande av handlingen, framställande av den elektroniska underskriften och arkivering hanteras i olika tekniska systemlösningar krävs att handlingen och underskriften behåller samma arkivformat, bevaras i ursprungligt skick, kontrolleras med checksumma genom rutiner och tekniska åtgärder under hela processen. Det innebär i praktiken att det krävs integrationer mellan systemlösningarna och noggranna tester för att säkerställa handlingens autenticitet och integritet. Det går annars inte att bevisa att handlingen och den elektroniska underskriften är i ursprungligt skick och helt intakt.

Generellt om beslutsprocess, informationssäkerhet och upphandling

Det finns flera regelverk och interna beslutsstrukturer att beakta vid införskaffande av funktionalitet för elektroniska underskrifter, precis som vid införskaffande av alla nya IS/IT-lösningar. Här följer en genomgång av några av de viktigaste kontrollpunkterna att ta hänsyn till.

IS/IT styrmodell

IS/IT styrmodell beskriver den övergripande strukturen och grunden för hur vi arbetar med IS/IT i Västra Götalandsregionen. Modellen beskriver hur vi ska fördela ansvar och fatta beslut, hur vi ska ställa krav och finansiera samt utveckla och utföra.

Styrmodellens struktur är baserad på objekt som är en samverkansarena för verksamhet och IT. Varje objekt hanterar mer specifika IT-funktioner och IT-stöd och ansvarar för att göra beställningar till utförare. Leverans av IS/IT sker alltid av eller via utföraren, VGR IT.

Den regionala berednings- och beslutsprocessen för IS/IT-utveckling utgår från beslutad IS/IT-styrmodell och syftar till ett gemensamt arbetssätt. Huvudmomenten i processen är ”att bedöma” och ”genomföra förstudie”.

Nya behov som ska beredas ska lägga in i verktyget Plexus. Stor andel av behoven kanaliseras via samordnare av IS (SIS) till respektive objekt som bedömer och bereder. Detta innebär att behov av elektroniska underskrifter ska initieras genom att behovet läggs in i Plexus.

För att beslut ska kunna fattas på gemensam grund har fem styrande principer fastslagits i styrmodellen IS/IT:

- kundnytta ska vara överordnad IS/IT
- helheten prioriteras före delarna
- för varje verksamhetsfunktion är strävan att det endast ska finnas en IS/IT-lösning
- vid anskaffning av IS/IT ska standardiserade produkter, tjänster eller lösningar vara huvudalternativet
- ge användaren tillgång till rätt tjänst, rätt information, vid rätt tillfälle, på rätt plats och på rätt sätt

För mer information om styrmodell och beredningsprocess:
https://insidan.vgregion.se/kontakt-och-organisation/regiongemensamma-kontaktuppgifter/ledning-och-styring-av-is-it/

Informationsklassning

En informationsklassning ska genomföras innan en tjänst för elektroniska underskrifter upphandlas eller tas i bruk eller om någon förändring sker när tjänsten är etablerad som kan påverka informationsbehandlingen. All information som hanteras i underskriftstjänsten ska genomgå informationsklassning. Syftet med informationsklassningen är att bedöma informationens skyddsnivå och skydda informationen på rätt sätt. Informationsklassningen ska ske utifrån generella säkerhetskrav och de specifika säkerhetskrav som ställs av verksamheten. En informationsklassning ger därför ett underlag för krav på fysiskt skydd, administrativa och tekniska skyddsåtgärder och ska dokumenteras. Resultatet används vid kravställning i samband med upphandling.

Se vidare Rutin för klassificering av information.

Risk- och sårbarhetsanalys

En risk- och sårbarhetsanalys ska genomföras för att bedöma om det är möjligt att använda elektroniska underskrifter för behandling av den tänkta informationslagringen. En risk- och sårbarhetsanalys ska genomföras innan en tjänst för elektroniska underskrifter upphandlas eller tas i bruk eller om någon förändring sker när tjänsten har etablerats som kan påverka informationsbehandlingen. Risker och sårbarheter ska löpande identifieras och analyseras, och ansvariga ska ta ställning till hur riskerna ska hanteras. Tänk på att en särskild konsekvensbedömning enligt GDPR även krävs i vissa fall (se information om konsekvensbedömning under avsnittet om personuppgiftshantering).

Se vidare Rutin för riskanalys.

Personuppgiftshantering

EU:s dataskyddsförordning (GDPR) ställer krav på myndigheter och andra organisationer när personuppgifter behandlas och syftar till att skydda den personliga integriteten. Nedanstående bestämmelser bör beaktas innan införandet

av nya digitala lösningar för elektroniska underskrifter och en analys bör göras av vilka krav som bör ställas i eventuell upphandling.

Personuppgiftsansvarig
Vid val av teknisk lösning för elektronisk underskrift, och vid eventuell användning av s k ”egna utrymmen”, måste säkerställas vilken myndighet som är personuppgiftsansvarig för personuppgiftsbehandlingen om användarna av tjänsten för elektronisk signering och om andra personer som kan förekomma i handlingen som ska skrivas under. Det behöver också säkerställas hur personuppgiftsansvaret fördelar sig i tjänsten mellan myndigheten och leverantören. Om t ex förlitandeavtal tecknas är det viktigt att klarlägga om leverantören av identitetsintyg har ett eget personuppgiftsansvar eller är ett personuppgiftsbiträde. Detta bör klarläggas utifrån omständigheterna i den enskilda tjänsten. Personuppgiftsansvarig har det yttersta ansvaret för att GDPR beaktas vid användning av elektroniska underskrifter. (För mer information om *eget utrymme* se eSams vägledning Eget utrymme hos myndighet – en vägledning.)

Fördelningen av personuppgiftsansvaret för legitimerings-, identifierings-, intygs- och underskriftsfunktioner har berörts av E-legitimationsnämnden. Där har personuppgiftsansvaret beskrivits så att det flyttas över stegvis när en transaktion flödar genom infrastrukturen. Detta synsätt, som avses gälla även för den särskilda övergångstjänsten, innebär att varje aktör är personuppgiftsansvarig för sitt led i hanteringen. (För mer information om hur personuppgiftsansvaret fördelar sig se eSams juridiska vägledning för införande av e-legitimering och e-underskrifter 1.1, s. 58.)

Registerförteckningen
Personuppgiftsbehandlingen som ska utföras i ny teknisk lösning för e-underskrift ska anges i den personuppgiftsansvariga myndighetens registerförteckning. I registerförteckningen dokumenteras för vilket ändamål personuppgifterna ska användas och hur GDPR:s regler efterlevs.

Informationsskyldigheten och de registrerades rättigheter
GDPR innehåller omfattande bestämmelser om den information som ska lämnas till de registrerade om hur personuppgifterna används och om de registrerades rättigheter (artikel 13-14). Informationen ska vara enkel att ta del av.

Det är den personuppgiftsansvariges ansvar att säkerställa att de registrerades rättigheter enligt GDPR kan tillgodoses i lösningen för elektronisk underskrift. Exempel på de registrerades rättigheter är rätten till tillgång till en kopia av sina personuppgifter.

Hantering av personnummer
I den svenska dataskyddslagen (SFS 2018:218), som kompletterar GDPR, finns särskilda bestämmelser om personnummer och samordningsnummer. Personnummer och samordningsnummer får, enligt 10 §, behandlas utan samtycke endast när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Säkerhetsåtgärder

Enligt artikel 32 GDPR ska lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig i förhållande till risken med beaktande av den senaste utvecklingen, genomförandekostnaderna, behandlingens art, omfattning sammanhang och ändamål.

Principen om ansvarsskyldighet i artikel 24 ställer, efter införande av GDPR, uttryckligt krav på att den personuppgiftsansvarige, ska kunna *visa* att kraven i GDPR efterlevs.

Principerna inbyggt dataskydd och dataskydd som standard innebär att den personuppgiftsansvarige bör välja den IT-lösning som ger de bästa tekniska förutsättningarna för dataskydd och ska även tillämpas vid upphandlingar.

Genom rätt säkerhetsåtgärder ska säkerställas att personuppgifter inte hanteras på ett felaktigt sätt, att obehöriga inte kan ta del av inlämnade uppgifter och framförallt att andra inte kan missbruka en persons e-underskrift så att innehavaren lider skada. En annan aspekt, lika viktigt för organisationen som för användaren, är att e-legitimationen och e-underskriften är utformad på ett sådant sätt att det med tillräckligt hög säkerhet går att identifiera den som ska använda exempelvis en e-tjänst. (se eSams vägledning sid 9).

För analys och val av säkerhetsåtgärder för personuppgifter tillämpas befintliga rutiner för informationsklassificering och riskanalys och bör uppdateras kontinuerligt. Resultatet av bedömningen av vilka säkerhetsåtgärder som är lämpliga bör beaktas vid kravställning i samband med upphandling.

Säkerställ även att rutiner för anmälan av eventuella personuppgiftsincidenter kan följas. Tydliggör i personuppgiftsbiträdesavtalet med leverantören vilka kontaktvägar som ska användas vid eventuella personuppgiftsincidenter.

Konsekvensbedömning
Enligt GDPR artikel 35.1 ska i vissa fall en särskild bedömning av behandlingens konsekvenser för skyddet för personuppgifter göras före behandlingen påbörjas. Konsekvensbedömningen ska göras om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Följ regionens rutin för konsekvensbedömning enligt GDPR.

Personuppgiftsbiträde
Om behandling av personuppgifter ska genomföras av ett personuppgiftsbiträde ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i GDPR och säkerställer att den registrerades rättigheter skyddas.

Ett personuppgiftsbiträdesavtal bör tecknas som motsvarar SKR:s rekommenderade avtalsvillkor. I upphandlingen ska personuppgiftsbiträdesavtalet ingå som en bilaga. Om leverantören anlitar underleverantörer som i sin tur behandlar personuppgifterna (s k “underbiträden”) krävs godkännande av VGR i SKR-mallen och aktuella underleverantörer ska listas i bilagan. Berörd leverantör

bör svara för sina underleverantörer som om leverantören hade utfört åtgärden själv.

IT-säkerhet/teknik

Efter utförd informationsklassificering och risk- och sårbarhetsanalys och eventuell konsekvensbedömning kommer det framgå vilken skyddsnivå informationen behöver ha. Med hjälp av informationsklassificeringen tar man fram upphandlingskrav och säkerhetskrav som ska uppfyllas av systemleverantören.

IT-säkerhetskrav för drift och underhåll utgår från Riktlinjer för Informationssäkerhet samt underliggande rutiner.

Upphandling

För att upphandla lösning för elektroniska underskrifter görs ansökan om upphandling i Marknadsplatsen och prioriteras utifrån resurser av Koncerninköp. Anskaffning hanteras därefter enligt inköpsprocessens tre steg (analys, upphandling och avtalsfas) där verksamhetsföreträdare deltar i kravställning utifrån verksamhetens behov samt även utifrån ett kostnadsperspektiv. Anskaffning av lösning kan ske via olika alternativ:

- Genom att VGR genomför en upphandling i enlighet med LOU
- Avrop genom förnyad konkurrensutsättning på Kammarkollegiets ramavtal
- Eventuellt avrop på befintligt avtal, dock förenat med riskexponering utifrån ett LOU-perspektiv
- Alternativt ansluta sig till Ineras signeringstjänst till en fast kostnad

Inköpsprocessen
Ansökan om upphandling

Checklista

1. Behöver de tänkta dokumenten underskrift?
2. Vilken funktion av underskriften ska hanteras elektroniskt?
3. Finns redan ett system som kan omhänderta behovet?
4. Har behovet gått genom ärendehanteringssystemet för IS/IT-styrmodell?
5. Har informationsägare utsetts?
6. Följer projektet projektmodellen Projektilen?
7. Finns finansiering för att säkerställa tjänsten?
8. Följer projektet VGR:s inköpsprocess?
9. Är informationsklassning genomförd?
10. Är risk- och sårbarhetsanalys genomförd?
11. Vilka säkerhetskrav har informationsklassning och risk- och sårbarhetsanalys identifierat och hur kan de omhändertas?
12. Är det klarlagt vilken styrelse/nämnd som är personuppgiftsansvarig för behandlingen?
13. Har det säkerställts att personuppgifter behandlas korrekt och har rätt säkerhetsåtgärder för personuppgifterna vidtagits?
14. Har en konsekvensbedömning enligt GDPR, om tillämpligt, genomförts?

15. Har nödvändiga personuppgiftsbiträdesavtal upprättats?
16. Vilken nivå av underskrift behövs?
17. Behöver tjänsten innefatta e-legitimering?
18. I så fall vilken nivå av e-legitimering?
19. Framställs handlingen och den elektroniska underskriften med arkivbeständiga format?
20. Kan handlingen och underskriften bevaras i ursprungligt skick i den tekniska lösningen?
21. Kan underskriftens giltighet fortsätta att valideras?