Gäller för: Västra Götalandsregionen
Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare
Godkänd av: Johan Flarup, (johfl), Direktör

Giltig från: 2024-08-05
Giltig till: 2028-07-24

Informationssäkerhet för extern molntjänst

Regional rutin 2024 – 2028

Ledningssystem för informationssäkerhet och dataskydd

VÄSTRA GÖTALANDSREGIONEN

Innehållsförteckning

Sammanfattning 3

1 Allmänt 4

1.1 Avgränsning 4

2 Risker 5

3 Personuppgifter, sekretess och annan skyddsvärd information 6

4 Säkerhetsåtgärder 6

4.1 Anskaffa extern molntjänst 6

4.2 Förvalta extern molntjänst 7

4.4 Lämna extern molntjänst 7

4.5 Förteckning av säkerhetsåtgärder 8

4 Relaterade dokument 15

Sammanfattning

Mål: *Västra Götalandsregionens informationstillgångar ska skyddas på ett likvärdigt sätt när tillgången hanteras av en extern leverantör.*

Regional rutin informationssäkerhet för användning av extern molntjänst specificerar och hanterar informationssäkerhet för området.

Rutinen är styrande för alla förvaltningar och bolag i Västra Götalandsregionen (VGR) och ingår i ledningssystemet för informationssäkerhet och dataskydd (LISD). Rutinen är utformad med stöd av VGR:s policy för säkerhet och beredskap samt riktlinje för informationssäkerhet och dataskydd.

I rutinen fastställs och beskrivs de säkerhetsåtgärder som ska vidtas när extern molntjänst anskaffas, förvaltas och när VGR lämnar eller avslutar informationsbehandling i en extern molntjänst. Säkerhetsåtgärderna utgår från svensk standard. Rutinen fastställer grundnivån för hur VGR hanterar risker mot informationssäkerhet förknippade med externa molntjänster.

1 Allmänt

Den huvudsakliga delen av rutinen är 4.5 Förteckning av säkerhetsåtgärder, övriga delar syftar till att ge läsaren stöd i att förstå tillämpning av säkerhetsåtgärderna som framgår i förteckningen. Förteckningen består av säkerhetsåtgärder för de informationssäkerhetsrisker som uppstår vid användning av extern molntjänst och omfattar inte säkerhetsåtgärder för risker utanför denna omfattning som normalt behöver vidtas oavsett om extern molntjänst eller inte används.

Det är viktigt att definiera vad en extern molntjänst är för att förstå när rutinen är tillämplig. Förenklat betyder extern molntjänst mjukvara eller hårdvara för databehandling som tillhandahålls över internet där resurserna för behandlingen inte är placerade hos eller hanteras av VGR eller något av VGR:s majoritetsägda bolag.

Standardiserade definitioner av begreppet *molntjänst* och *molnbaserad databehandling*[1] ligger till grund för rutinens definition.

1.1 Avgränsning

Rutinen specificerar inte säkerhetsåtgärder utifrån alla tänkbara krav som framgår av lagar, förordningar och föreskrifter på detaljnivå men belyser huvudsakliga områden. Juridiska bedömningar görs i samband med informationsklassnings- och riskhanteringsprocessens genomförande.

[1] Online Browsing Platform (OBP) (iso.org)

2 Risker

Vid användning av extern molntjänst uppstår ett antal risker. Dessa omfattar bland annat:

- På grund av att data behandlas med hjälp av IT-utrustning som molntjänstleverantören hanterar finns det risk att obehöriga får åtkomst till VGR:s informationstillgångar vilket kan leda negativa konsekvenser för VGR:s verksamheter, ekonomi, förtroende och enskildas personliga integritet.

- På grund av det delade ansvaret som uppstår mellan VGR, molntjänstleverantören och eventuella underleverantörer för informationssäkerhet och dataskydd vid användning av extern molntjänst finns det risk att informationstillgångarna inte skyddas på ändamålsenligt sätt vilket kan leda till bristande informationssäkerhet och i förlängningen negativa konsekvenser för VGR:s verksamheter, ekonomi, förtroende och enskildas personliga integritet.

- På grund av användning av delade virtuella informationsbehandlingsresurser finns det risk att obehöriga får åtkomst till VGR:s informationstillgångar vilket kan leda negativa konsekvenser för VGR:s verksamheter, ekonomi, förtroende och enskildas personliga integritet.

- På grund av olika juridiska risker som uppstår bland annat eftersom olika länder har sina egna lagstiftningar som inte alltid stämmer överens med svensk lag finns det risk att VGR bryter mot svensk lag vilket kan leda till negativa konsekvenser för VGR:s verksamheter, ekonomi, förtroende och enskildas personliga integritet.

3 Personuppgifter, sekretess och annan skyddsvärd information

Att hantera informationstillgångar som omfattas av sekretess eller som av andra anledningar är extra skyddsvärda i en extern molntjänst innebär extra noggranna förberedelser och analyser av den aktuella molntjänstens förmåga och förutsättningar att efterleva tillämplig lag och informationssäkerhetskrav. Därtill ska alltid förutsättningarna utvärderas att välja en on-premise lösning, det vill säga en lösning som installeras och hanteras av VGR.

4 Säkerhetsåtgärder

De säkerhetsåtgärder som framgår i denna rutin utgör grundnivån för informationssäkerhet och dataskydd för användning av extern molntjänst. Det betyder att dessa säkerhetsåtgärder alltid ska tillämpas oavsett om risk identifierats eller inte. Det är alltså möjligt att säkerhetsåtgärd vidtas med begränsad eller ingen effekt men att detta är acceptabelt.

Det har ingen betydelse om databehandlingen enbart avser överföring till molntjänstleverantör men inte lagring så som för strömmande data. Säkerhetsåtgärderna ska användas även när information inte lagras hos molntjänsteleverantör.

Säkerhetsåtgärderna är indelade i tre olika faser (anskaffa, förvalta och lämna) av en tjänsts livscykel för att underlätta identifiering av ansvar för implementation och uppföljning i motsvarande process inom VGR.

4.1 Anskaffa extern molntjänst

I processen för anskaffning finns möjlighet att hantera ett antal av de risker som uppstår. Det är i denna process VGR ska ställa de krav som behövs för informationssäkerhet och dataskydd. Kraven omfattar molntjänstleverantörens verksamhet och de produkter och tjänster som erbjuds.

Det är övervägande flest säkerhetsåtgärder som behöver beaktas i just anskaffningsfasen även om implementationen eller uppföljning inte alltid sker här.

4.1.1 Informationsklassning

Informationstillgångarna som avses hanteras ska före anskaffning klassas i enlighet med gällande regional rutin (säkerhetsåtgärd 24):

VGR ska definiera krav på informationssäkerhet och dataskydd genom fastställd informationsklassning för informationstillgångarna som avses

behandlas och utvärdera om de tjänster som erbjuds av molntjänstleverantör uppfyller dessa krav...

Klassning är en förutsättning för ändamålsenlig informationssäkerhet och dataskydd. Det är vid informationsklassning som de legala kraven identifieras, inte enbart vilken lag, förordning eller föreskrift som är tillämplig. De legala kraven ligger till grund för anskaffning och om hanteringen är förenlig med svensk lag.

Särskilt viktiga krav att identifiera i för anskaffning av extern molntjänst är krav på geografisk placering/länder där informationstillgångar kan hanteras och krav på ägarförhållande med hänsyn till andra länders jurisdiktion.

4.1.2 Riskhantering

Grundläggande utöver informationsklassning för att identifiera nödvändiga säkerhetsåtgärder är också riskarbetet (säkerhetsåtgärd 42):

VGR ska genomföra riskanalys som omfattar risker mot informationssäkerhet och dataskydd för den tänkta hanteringen...

Eventuella kvarstående risker kopplade till användningen av molntjänsten ska tydligt identifieras och godkännas av den som äger risken.

4.2 Förvalta extern molntjänst

Under förvaltningsfasen av extern molntjänst är det inte bara ansvarsfrågan som är viktig utan även uppföljning, utbildning, riskhantering, kapacitetsplanering, säkerhetskopiering, loggning och andra säkerhetsåtgärder som behöver tas omhand, exempelvis (säkerhetsåtgärd 17):

VGR:s förändringsprocess ska ta hänsyn till konsekvenserna av ändringar som görs av molntjänstleverantören.

4.4 Lämna extern molntjänst

Åtgärderna syftar till att säkerställa att information inte lämnas kvar hos leverantör, att informationstillgångar återlämnas till VGR i ett hanterbart format och att hanteras på ett sätt som möter verksamheternas krav.

4.5 Förteckning av säkerhetsåtgärder

Förteckning av säkerhetsåtgärder är den huvudsakliga delen av rutinen. Vissa av säkerhetsåtgärderna ska alltid tillämpas, oavsett typ av tjänst eller tänkt informationshantering medan andra har villkor för tillämpning. Villkoren baseras på informationsklass, om informationstillgångarna omfattas av sekretess eller utgör personuppgifter.

I förteckningen av säkerhetsåtgärder framgår följande i kolumnföljd:

ID, identifierare för respektive säkerhetsåtgärd.

K/R/T/S/P, kriterier för säkerhetsåtgärdens tillämpning. Konfidentialitet (K), riktighet (R) eller tillgänglighet (T) är markerat med den lägsta informationsklass[2] då säkerhetsåtgärden ska tillämpas. Sekretess (S) och personuppgifter (P) avser om hanteringen omfattar information med sekretess eller personuppgifter och är markerat med "X" då säkerhetsåtgärden ska tillämpas. Säkerhetsåtgärden är obligatorisk om ett eller flera av kriterierna uppfylls.

Säkerhetsåtgärd, beskrivning av säkerhetsåtgärd som ska vidtas om ett av kriterierna möts.

ANS/FÖR/LÄMNA, indikerar om säkerhetsåtgärden behöver beaktas, implementeras och följas upp när VGR anskaffar (ANS), förvaltar (FÖR) och lämnar (LÄMNA).

[2] Enligt klassningsmodell i regional rutin informationsklassning

ID	K	R	T	S	P	Säkerhetsåtgärd	ANS	FÖR	LÄMNA	Referens
1	**0**	**0**	**0**	**X**	**X**	Fördelning av roller och ansvar avseende informationssäkerhet och dataskydd för både VGR och molntjänsteleverantören ska anges i avtal med hänsyn till vilken typ av molntjänst det rör sig om. Till exempel kan fördelningen av ansvaret för säkerhetsåtgärder av applikationsskiktet skilja sig åt beroende på om molntjänstleverantör tillhandahåller en SaaS-tjänst i förhållande till en PaaS- eller IaaS-tjänst där VGR kan bygga eller lägga upp sina egna applikationer. VGR ska bekräfta dessa roller och ansvarsområden som kan omfatta: • skydd mot skadlig kod; • säkerhetskopiering; • kryptografiska säkerhetsåtgärder; • hantering av sårbarheter; • hantering av incidenter; • kontroll av teknisk överensstämmelse; • säkerhetstestning; • revision; • insamling, underhåll och skydd av bevis, inklusive loggar; • skydd av information vid uppsägning av avtalet; • autentisering och åtkomstkontroll; • identitets- och åtkomsthantering.	**X**			SS-EN ISO/IEC 27017:2021 6.1.1 SS-EN ISO/IEC 27017:2021 15.1.2 SS-EN ISO/IEC 27017:2021 16.1.1 SS-EN ISO/IEC 27018:2020 5.1.1 SS-EN ISO/IEC 27018:2020 16.1
2	**0**	**0**	**0**	**X**	**X**	VGR ska identifiera och hantera sin relation med kundsupport hos molntjänsteleverantören.		**X**		SS-EN ISO/IEC 27017:2021 6.1.1
3	**0**	**0**	**0**	**X**	**X**	VGR ska identifiera de jurisdiktioner som är relevanta för VGR och molntjänstleverantörens kombinerade verksamhet. Information om geografiska platser där uppgifter kan lagras, behandlas eller överföras till kan underlätta att fastställa tillsynsmyndigheter och jurisdiktioner.	**X**			SS-EN ISO/IEC 27017:2021 6.13
4	**0**	**0**	**0**	**X**	**X**	VGR ska tillhandahålla utbildning till chefer och ansvariga för molntjänster, molntjänstadministratörer, molntjänstintegratörer och molntjänstanvändare, inklusive relevanta anställda och konsulter.		**X**		SS-EN ISO/IEC 27017:2021 7.2.2
5	**0**	**0**	**0**	**X**	**X**	VGR:s inventering av tillgångar ska redogöra för informationstillgångar som lagras i extern molntjänst. I inventarieförteckningen ska det anges var tillgångarna förvaras.		**X**		SS-EN ISO/IEC 27017:2021 8.1.1
6	**0**	**0**	**0**			IT-säkerhetsspecifikationen för den externa molntjänsten ska specificera kraven för åtkomst till tjänsten.		**X**		SS-EN ISO/IEC 27017:2021 9.1.2

ID	K	R	T	S	P	Säkerhetsåtgärd	ANS	FÖR	LÄMNA	Referens
7	**0**	**0**	**0**			VGR ska använda tillräckliga autentiseringstekniker (t.ex. flerfaktorsautentisering) för att autentisera molntjänstadministratörer till molntjänstens administrativa funktioner i enlighet med de identifierade riskerna.	**X**	**X**		SS-EN ISO/IEC 27017:2021 9.2.3
8	**0**	**0**	**0**			I de fall molntjänstleverantörens tilldelar autentiseringsinformation, t.ex. lösenord ska VGR kontrollera att hanteringen uppfyller VGR:s krav.	**X**			SS-EN ISO/IEC 27017:2021 9.2.4
9	**0**	**0**	**0**			VGR ska se till att åtkomsten till information i molntjänsten kan begränsas i enlighet med gällande styrande dokument och att sådana begränsningar förverkligas.	**X**	**X**		SS-EN ISO/IEC 27017:2021 9.4.1
10	**0**	**0**	**0**			VGR ska i de fall molntjänstmiljön omfattar ytterligare områden, exempelvis virtualiseringsfunktioner, databashanterare och administrativa applikationer utvärdera och vid behov tillämpa ytterligare åtkomstkontroll.	**X**	**X**		SS-EN ISO/IEC 27017:2021 9.4.1
11	**0**	**0**		**X**	**X**	VGR ska använda kryptografiska säkerhetsåtgärder för sin användning av molntjänsten. Säkerhetsåtgärderna ska vara tillräckligt kraftfulla för att minska de identifierade riskerna. VGR ska begära information från molntjänstleverantören om de situationer där kryptering används för att skydda de uppgifter som behandlas samt eventuella funktioner som kan hjälpa VGR att tillämpa egen kryptografiskt skydd.	**X**			SS-EN ISO/IEC 27017:2021 10.1.1 SS-EN ISO/IEC 27018:2020 10.1.1
12	**0**	**0**	**0**			När molntjänstleverantören erbjuder kryptografiska säkerhetsåtgärder ska VGR granska all information som tillhandahålls av molntjänstleverantören för att bekräfta att de kryptografiska funktionerna: • uppfyller informationsklassningens krav; • är kompatibla med andra kryptografiska skydd som används av VGR.	**X**	**X**		SS-EN ISO/IEC 27017:2021 10.1.1
13	**0**	**0**	**0**			VGR ska identifiera krypteringsnycklar för molntjänsten och införa rutiner för nyckelhantering.		**X**		SS-EN ISO/IEC 27017:2021 10.1.2
14	**0**	**0**	**0**	**X**	**X**	VGR ska om molntjänstleverantören tillhandahåller nyckelhanteringsfunktionalitet för molntjänsten begära följande information: • Typ av krypteringsnycklar som används; • Specifikationer för nyckelhanteringen, inklusive varje steg i nycklarnas livscykel (generering, registrering, säkerhetskopiering, distribution, installation, användning, förnyelse, lagring, destruktion); • Rekommenderade nyckelhanteringsrutiner som VGR kan användas.	**X**			SS-EN ISO/IEC 27017:2021 10.1.2
15	**0**	**0**	**0**	**X**	**X**	VGR ska inte tillåta att molntjänstleverantören lagrar och hanterar krypteringsnycklar för kryptografiska operationer när VGR använder egen eller en separat nyckelhanteringstjänst.	**X**	**X**		SS-EN ISO/IEC 27017:2021 10.1.2

ID	K	R	T	S	P	Säkerhetsåtgärd	ANS	FÖR	LÄMNA	Referens
16	**0**	**0**	**0**	**X**	**X**	VGR ska bekräfta att molntjänstleverantören har rutiner för säker avveckling och återanvändning av hårdvara.	**X**	**X**		SS-EN ISO/IEC 27017:2021 11.2.7
17	**1**		**2**	**X**	**X**	VGR:s förändringsprocess ska ta hänsyn till konsekvenserna av ändringar som görs av molntjänstleverantören.		**X**		SS-EN ISO/IEC 27017:2021 12.1.2
18			**2**			VGR ska se till att den överenskomna kapacitet som tillhandahålls av molntjänsten uppfyller VGR:s krav. VGR ska övervaka användningen av molntjänsten och prognostisera kapacitetsbehov för att säkerställa molntjänstens prestanda över tid.	**X**	**X**		SS-EN ISO/IEC 27017:2021 12.1.3
19	**1**		**1**	**X**	**X**	VGR ska begära specifikationer för säkerhetskopiering från molntjänstleverantören samt kontrollera att de uppfyller VGR:s krav. VGR ska implementera säkerhetskopiering när molntjänstleverantören inte tillhandahåller det.	**X**	**X**		SS-EN ISO/IEC 27017:2021 12.3.1
20	**2**	**1**		**X**	**X**	VGR ska definiera krav på händelseloggning och kontrollera att molntjänsten uppfyller dessa krav.	**X**	**X**		SS-EN ISO/IEC 27017:2021 12.4.1
21	**0**	**0**	**0**	**X**	**X**	VGR ska definiera krav på synkronisering av tid för molntjänstleverantörens system. Utan en sådan synkronisering kan det vara svårt att stämma av händelser i VGR:s system med händelser i molntjänstleverantörens system.	**X**			SS-EN ISO/IEC 27017:2021 12.4.4
22	**0**	**0**	**0**	**X**	**X**	VGR ska begära information från molntjänstleverantören om hanteringen av tekniska sårbarheter som kan påverka molntjänsten och identifiera de tekniska sårbarheter som VGR kommer att ansvara för att hantera.	**X**	**X**		SS-EN ISO/IEC 27017:2021 12.6.1
23	**2**	**1**	**1**	**X**	**X**	VGR ska definiera krav för nätverkssegmentering för att uppnå isolering i molntjänstens delade IT-miljö och kontrollera att molntjänstleverantören uppfyller dessa krav.	**X**			SS-EN ISO/IEC 27017:2021 13.1.3
24	**0**	**0**	**0**	**X**	**X**	VGR ska definiera krav på informationssäkerhet och dataskydd genom fastställd informationsklassning för informationstillgångarna som avses behandlas och utvärdera om de tjänster som erbjuds av molntjänstleverantör uppfyller dessa krav. Informationsklassningen ska, men inte begränsat till innehålla: • krav på geografisk placering dit informationstillgången får föras över och behandlas; • krav på den som utför behandlingen eller tillhandahåller informationsbehandlingsresurserna.	**X**			SS-EN ISO/IEC 27017:2021 14.1.1
25	**1**	**1**	**1**	**X**	**X**	VGR ska begära information från molntjänstleverantören om hur molntjänstleverantören använder säkra utvecklingsrutiner och metoder.	**X**			SS-EN ISO/IEC 27017:2021 14.2.1

ID	K	R	T	S	P	Säkerhetsåtgärd	ANS	FÖR	LÄMNA	Referens
26	**0**	**0**	**0**	**X**	**X**	VGR ska begära information från molntjänstleverantören om rutiner för: • rapportering av informationssäkerhetshändelser till molntjänstleverantören; • möjlighet att följa statusen för en rapporterad informationssäkerhetshändelse; • rapportering av informationssäkerhetshändelser som upptäcks av molntjänstleverantören.	**X**	**X**		SS-EN ISO/IEC 27017:2021 16.1.2
27	**0**	**0**	**0**	**X**	**X**	VGR ska beakta lagar och förordningar som gäller för molntjänstleverantören och begära bevis på att molntjänstleverantören följer relevanta bestämmelser och standarder som krävs för VGR:s verksamhet. Sådana bevis kan vara certifieringar från tredjepartsrevisorer.	**X**			SS-EN ISO/IEC 27017:2021 18.1.1
28	**0**	**0**	**0**	**X**	**X**	VGR ska ha rutiner för att identifiera molnspecifika licenskrav före licensierad programvara installeras i extern molntjänst. Särskild uppmärksamhet ska ägnas åt fall där molntjänsten är skalbar och programvaran kan köras på fler system eller processorkärnor än vad licensvillkoren tillåter. Installation av kommersiellt licensierad programvara i en molntjänst kan leda till brott mot licensvillkoren för programvaran.	**X**	**X**		SS-EN ISO/IEC 27017:2021 18.1.2
29	**0**	**0**	**0**	**X**	**X**	VGR ska verifiera att den uppsättning kryptografiska säkerhetsåtgärder som används av en molntjänst överensstämmer med relevanta avtal, lagar och förordningar.	**X**			SS-EN ISO/IEC 27017:2021 18.1.5
30	**2**			**X**	**X**	VGR ska begära dokumenterade bevis för att implementation av säkerhetsåtgärder stämmer med molntjänstleverantörens påståenden. Sådana bevis kan vara certifieringar från tredjepartsrevisorer.	**X**			SS-EN ISO/IEC 27017:2021 18.2.1 SS-EN ISO/IEC 27018:2020 18.2.1
31					**X**	VGR ska begära att molntjänstleverantören utser en kontaktpunkt avseende personuppgiftsbehandlingen enligt avtalet.	**X**	**X**		SS-EN ISO/IEC 27018:2020 6.1.1
32					**X**	VGR ska begära att molntjänstleverantörens medarbetare är medvetna om möjliga konsekvenser för den egna organisationen, den personuppgiftsansvarige och registrerade vid bristfällig efterlevnad av regler och hantering av personuppgifter.	**X**			SS-EN ISO/IEC 27018:2020 7.2.2
33					**X**	VGR ska för säker avveckling eller återanvändning av utrustning som innehåller lagringsmedia och eventuellt kan innehålla personuppgifter behandla dessa som att de innehåller personuppgifter.	**X**	**X**	**X**	SS-EN ISO/IEC 27018:2020 11.2.7
34				**X**	**X**	VGR ska ha rutiner för att granska händelseloggar med en specificerad periodicitet för att identifiera oegentligheter. För detta behöver VGR säkerställa att molntjänstleverantören samlar in ändamålsenliga loggar, exempelvis innehållande vilka förändringar som gjorts och av vem.	**X**	**X**		SS-EN ISO/IEC 27018:2020 12.4.1 (27002 8.15)
35	**2**			**X**	**X**	VGR ska definiera för vem, när och hur logginformation görs tillgänglig eller användas.	**X**	**X**		SS-EN ISO/IEC 27018:2020 12.4.1

ID	K	R	T	S	P	Säkerhetsåtgärd	ANS	FÖR	LÄMNA	Referens
36					**X**	VGR ska säkerställa ändamålsenlig åtkomstkontroll till logginformation för ändamål så som säkerhetsövervakning och driftdiagnostik.	**X**	**X**		SS-EN ISO/IEC 27018:2020 12.4.2
37					**X**	En informationssäkerhetsincident ska starta en granskning för att avgöra om ett dataintrång som omfattar personuppgifter har ägt rum. En informationssäkerhetshändelse behöver inte nödvändigtvis leda till en granskning. En informationssäkerhetshändelse är en händelse som inte resulterar i faktisk, eller betydande sannolikhet för obehörig åtkomst till personuppgifter eller till någon av molntjänstleverantörens utrustning eller anläggningar som lagrar personuppgifter och kan inkludera portscanningar, misslyckade inloggningsförsök, överbelastningsattacker och paketsniffning.	**X**	**X**		SS-EN ISO/IEC 27018:2020 16.1.1
38	**0**	**0**	**0**	**X**	**X**	VGR ska i de fall där tillsyn av molntjänstleverantörens leverans är opraktiskt eller kan öka säkerhetsriskerna begära att molntjänstleverantören tillhandahåller oberoende bevis på att informationssäkerheten hanteras i enlighet med VGR:s krav under hela avtalstiden.	**X**	**X**		SS-EN ISO/IEC 27018:2020 18.2.1
39				**X**	**X**	VGR ska där användning av externa molntjänst innebär att uppgifterna blir tillgängliga för molntjänsteleverantören säkerställa att: • Särskilt utpekade arbetstagare hos molntjänstleverantören är behöriga att ta del av uppgifterna genom att dessa personer knyts till VGR genom särskilda förordnanden så att de anses delta i verksamheten på lika villkor de egna anställda och under samma arbetsledning; eller • avtalsreglerad tystnadsplikt tecknas med arbetstagare hos molntjänstleverantören med åtkomst till uppgifterna; eller • uppgifterna är krypterade med godtagbart krypto vilket förutsätter att inte krypteringsnyckeln lämnas ut till molntjänstleverantören.	**X**	**X**		Sveriges Kommuner och Regioner Molntjänster och konfidentialitetsbedömning (skr.se)
40	**0**	**0**	**0**	**X**	**X**	VGR ska säkerställa att det i avtalet med molntjänstleverantören framgår att informationen ska återlämnas till VGR och raderas hos molntjänstleverantören när avtalet upphör. Molntjänstleverantören får efter avslutat avtal inte ha kvar någon del av den information som har behandlats för molntjänstleverantörens uppdrag om så inte framgår av avtal.	**X**		**X**	
41	**0**	**0**	**0**	**X**	**X**	Den myndighet inom VGR som anskaffar extern molntjänst för att hantera allmänna handlingar ska säkerställa att arkivlagens krav på bevarande och gallring beaktas (avser även loggar). Detta omfattar bland annat att: • handlingar gallras när de nått gallringsfristen i gällande bevarande- och gallringsbeslut;	**X**	**X**	**X**	SS-EN ISO/IEC 27018:2020 12.4.2

ID	K	R	T	S	P	Säkerhetsåtgärd	ANS	FÖR	LÄMNA	Referens
						• möjlighet att exportera handlingar i godkända format för fortsatt bevarande i myndighetens digitala arkiv; • handlingar kan raderas i samband med avvecklingen av molntjänsten.				
42	**0**	**0**	**0**	**X**	**X**	VGR ska genomföra riskanalys som omfattar risker mot informationssäkerhet och dataskydd för den tänkta hanteringen. Riskanalysen ska uppdateras vid förändrad funktionalitet samt vid förändrad användning av molntjänsten. Riskhantering ska genomföras före VGR:s informationstillgångar hanteras av molntjänsten.	**X**	**X**	**X**	

4 Relaterade dokument

Termbank för informationssäkerhet - nationell terminologi för informations- och cybersäkerhetsområdet

Policy för säkerhet och beredskap i Västra Götalandsregionen

Regional riktlinje för informationssäkerhet och dataskydd

Informationssäkerhet, cybersäkerhet och integritetsskydd - Kontroller av informationssäkerhet (ISO/IEC 27002:2022)

Informationsteknik - Säkerhetstekniker - Riktlinjer för säkerhetsåtgärder för molntjänster baserade på SS-EN ISO/IEC 27002 (ISO/IEC 27017:2015)

Informationsteknik - Säkerhetstekniker - Riktlinjer för skydd av personuppgifter i publika molntjänster som hanterar personuppgifter (ISO/IEC 27018:2019)

Sveriges Kommuner och Regioner, Molntjänster och konfidentialitetsbedömning (skr.se)

Information om handlingen

Handlingstyp: Rutin

Gäller för: Västra Götalandsregionen

Innehållsansvar: Robert Kielén, (robki1), Regionutvecklare

Godkänd av: Johan Flarup, (johfl), Direktör

Dokument-ID: RS10162-1596316381-126

Version: 3.0

Giltig från: 2024-08-05

Giltig till: 2028-07-24