Support Portal | Registry Services

Vilka frågor gällande dataskydd, IT-säkerhet och diverse rutiner behöver besvaras i samband med en registraransökan?

Agent - 2024-06-03 - Bli registrar

Nedan frågor gällande dataskydd, IT-säkerhet och diverse rutiner kommer att skickas till den sökande efter att ansökningsformuläret är mottaget och ansökningsavgiften är betald. Svaren på frågorna utgör en del av ansökan och ingår i den helhetsbedömning som görs om en ansökan godkänns eller inte. Komplettering till svaren kan komma att begäras in.

Diverse rutiner

1. För att vara registrar ska minst två medarbetare ha genomgått utbildning i form av studiematerial och domänkunskapskurser samt uppdatera sig regelbundet vid förändringar. Innan ni blir aktiverad registrar behöver dessa personer ha genomgått utbildningen.och ni kommer behöva delge oss datum för när det utfördes.Ange namn och mailadress till de två person hos er som kommer att genomgå utbildningen.

2. Registraren ska kontrollera att det är innehavaren som har begärt en registreringstjänst innan denna tjänst utförs. Beskriv hur ni identifierar kunden samt hur detta dokumenteras.

3. Hur kontrollerar ni riktigheten i kundens kontaktuppgifter innan de skickas till Internetstiftelsen. Hur kommer era rutiner se ut för att se till att dessa hålls uppdaterade mot vårt register? (Vi utför regelbundna kontroller för att se att informationen i vårt register är uppdaterat med korrekta och valida uppgifter)

4. Som registrar åt .se och .nu får man inte ha domäner registrerade på sig själv om de inte används i verksamheten, så kallad förbud mot lagerhållning. Det är även förbud mot uthyrning och försäljning av domäner i eget syfte. Har någon i er styrelse/anställda ett flertal domäner registrerade på er själva eller bolag som tillhör någon av er? Under .se/.nu eller andra tld:er. Om ja, är de registrerade i syfte att hyra ut eller sälja? Om de inte är registrerade i detta syfte, i vilket syfte är de då registrerade?

5. Kommer registrering av domännamn ske av kund direkt via er?

6.Kommer ni som registrar använda er av återförsäljare (subregistrarer)? "Om ni svarat ja till användning av återförsäljare (subregistrarer) är det alltid ni som registrar som ansvarar fullt ut för återförsäljarnas handlande gällande domännamn och registreringstjänster enligt registraravtalet. Detta innebär bland annat att ni som registrar ansvarar för att eventuella brister åtgärdas. Om inte det sker kan sanktioner utövas mot er som registrar då det är ni som är Internetstiftelsens avtalspart och Internetstiftelsen inte har något avtal med återförsäljaren (subregistraren).

För att förtydliga vad som menas med ett sådant ansvar följer här ett par exempel:

- Registraren ska hålla återförsäljare och dess personal informerade om regler/villkor för .se och .nu samt ändringar av dessa

- Återförsäljaren får inte ha andra regler, villkor eller hantering av registreringstjänsterna för .se och .nu än de som finns i avtalet mellan registrar och Internetstiftelsen. T.ex. att kund inte kan återaktivera domännamn efter förfallodatum, att auktoriseringskoders tecken inte är kompatibla med registryts system etc.

- Återförsäljaren behöver ha en kundtjänst som tillhandahåller fullgod support mot slutkund.

- Obligatoriska innehavaruppgifter behöver tas in av återförsäljaren för att kunna validera dessa innan de skickas vidare till registryt via registraren.

- Återförsäljaren behöver kunna hantera och veta hur överlåtelser till nya innehavare sker på säkert sätt och ha rutiner och ta in underlag som styrker detta.
- Återförsäljaren är en förlängd arm av en registrar och ska inte vara till för att agera anonymiseringstjänst.

  Vänligen bekräfta att ni förstått innebörden av detta. Beskriv även hur ert system är uppbyggt kring återförsäljare och hur er lösning ser ut för att kunna hjälpa kunder som ligger hos era återförsäljare i de fall en återförsäljare skulle missköta sig och bryta mot avtalet.

8. Registrarens webbsida ska ha tydliga instruktioner om hur registreringstjänsterna hanteras av registraren, såsom förnyelse, transfers, begäran om authkod, ägarbyte, ompekningar, byte av DS-poster etc. Vänligen bekräfta att ni förstått innebörden av detta. Innan ni blir aktiverad registrar behöver ni inkomma med länkar som leder till denna information på er webbsida.

9. Registrarens webbsida ska ha tydlig information om hur abuse kan rapporteras och hanteras. Innan ni bli aktiverad registrar behöver ni inkomma med länk som leder till denna information på er webbsida.

10.Abuse- och supportärenden behöver hanteras inom samma tidsintervall som registreringstjänster, det vill säga inom 5 dagar. Bekräfta att ni kan uppfylla detta kravet.

11.Vilken typ av verksamhet bedriver ni idag i det företag som ansöker om att bli registrar?

12.Har ni fler bolag vilka typer av verksamheter bedrivs i dessa?

Dataskydd

1.Finns antagna policy-dokument (externt publicerade såväl som interna styrdokument) över behandling av personuppgifter för kunder samt leverantörer/samarbetspartners?

2.För verksamheten register över personuppgifter som behandlas?

3.Anlitar verksamheten personuppgiftsbiträden för personuppgiftsbehandling?

4.Om JA: Har verksamheten ingått skriftliga personuppgiftsbiträdesavtal med samtliga personuppgiftsbiträden?

5.Redogörelse över rutiner vid, och säkerställande av, registrerades rättigheter enligt GDPR (information/registerutdrag, rättelse och radering, begränsning av behandling, dataportabilitet, invändning mot behandling, automatiserat beslutsfattande och profilering (t.ex. vid fakturaköp));

6.Har verksamheten rutiner vid personuppgiftsincident?

IT-säkerhet

1.Policy, ansvar, organisation

- Finns det ett fungerande ledningssystem för informationssäkerhet som fastställts av ledningen? Är det spritt i organisationen?
- Finns det personer med utpekat ansvar och befogenheter?
- Har ledningen avsatt resurser för att säkerställa att informations- och cybersäkerhetsarbetet kan genomföras i den omfattning som behövs?

2.Säkerhetsgranskningar/penetrationstester/kodgranskningar

- Vilka åtgärder har verksamheten vidtagit för att uppnå en relevant nivå för sina it-system och använder man vedertagna it-säkerhetsåtgärder?
- Företas regelbundna säkerhetsgranskningar? Andra externa kontroller?

3.Riskanalyser

- Har verksamheten ett systematiskt och riskbaserat arbetssätt för att skapa förutsättningar att skydda informationstillgångar även vid kriser och vid höjd beredskap? Finns det någon process för bedömning av informationssäkerhetsrisker? Hur ser riskbilden ut?

4.Incidenthantering/-rapportering

- Finns det rutiner för incidenthantering och -rapportering? Hur väl är den kommunicerad i organisationen?

5.Informationssäkerhetsinstruktioner

- Finns det informationssäkerhetsinstruktioner för medarbetare i verksamheten och ges det regelbunden utbildning?

6.Kontinuitetsplaner

- Finns det en kontinuitetsplan och när antogs den senaste av ledningen?