Datum
2018-03-15

Antal sidor
24

Allmänna riktlinjer för hantering av personuppgifter i Torsby kommun

Innehållsförteckning

1 Definitioner

1.1 Personuppgift

All slags information som direkt eller indirekt kan knytas till en (fysisk) person som är i livet är en personuppgift. Uppgiften kan enskilt eller i kombination med andra upplysningar knytas till en levande person om man av den registrerade uppgiften kan förstå vem det handlar om.

Exempel på direkta personuppgifter är namn, personnummer, födelsedatum och fotografier medan IP-adress, fastighetsbeteckning, kontonummer och användar-ID är exempel på indirekta personuppgifter. Tänk på att även initialer och annan typ av krypterad eller kodad information kan vara en personuppgift om man med hjälp av anslutande uppgifter kan förstå vem det rör sig om.

1.2 Behandling av personuppgift

I GDPR talar man om att personuppgifter behandlas. Med behandling menas allt som görs med personuppgifterna. Det kan exempelvis röra sig om insamling av personuppgifter, likaså registrering, lagring och spridning. Lagringen kan ske till exempel lokalt på din dator, på en samarbetsyta eller en server. Här följer en del exempel på vanliga behandlingar av personuppgifter:

- Kund- och leverantörsregister (kontaktpersoner och enskilda näringsidkare)
- Elektroniska besöksliggare och passersystem
- Filmer, bilder och foton av alla de slag, på anställda såväl som enskild privatperson
- Ekonomisystem, ärendehanteringssystem och övriga verksamhetssystem
- Pensionslistor
- Medarbetarsamtal, lönesamtal och utvärderingar av verksamheten (på individnivå)
- Kontaktinformation till kolleger så som intern telefonkatalog och kontakter i epostsystemet
- Behörighetsadministration och behandlingshistorik (loggar)
- GISar (Geografiska InformationsSystem - kan vara på individnivå)
- Kameraövervakning
- Spontanansökningar, rekryteringsdatabaser, kompetensdatabaser, personlighetstester/profiler
- Intranät och publik hemsida
- Egen registerförteckning - till exempel systemägare och kontaktperson för registerutdrag.
- Växelns IT-system lagrar ofta information om vem (vilken anknytning) som har ringt till vem och när

- System som inte längre används.

1.3 Känsliga personuppgifter

I GDPR finns ett generellt förbud att registrera känsliga personuppgifter. Bestämmelsen betyder inte att det är helt förbjudet att registrera känsliga personuppgifter, men utgångspunkten är att det är förbjudet och att man därför måste hitta ett undantag i GDPR för att det ska vara tillåtet. Känsliga personuppgifter definieras som:

- Ras eller etniskt ursprung (exempelvis uppgifter om modersmål, födelseland eller tolkbehov)
- Politiska åsikter (exempelvis medlemskap i politiskt parti)
- Religiös eller filosofisk övertygelse (exempelvis medlem i religiöst samfund, särskilda önskemål om mat eller andra behov som har religiös koppling)
- Medlemskap i fackförening,
- Hälsoinformation (exempelvis sjukfrånvaro, behov av hjälpmedel pga funktionsnedsättning eller placering i särskoleklass)
- Sexualliv (inklusive uppgifter om sexuell läggning)

I nya dataskyddsförordningen tillkommer ytterligare kategorier av känsliga personuppgifter:

- Genetiska uppgifter (uppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken, som kan framgå genom exempelvis dna-analys)
- Biometriska uppgifter (uppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken som erhållits genom en särskild teknisk behandling, exempelvis fingeravtryck)

1.4 Extra skyddsvärda personuppgifter

Datainspektionen har gjort en distinktion mellan känsliga personuppgifter (ovan stycke) och andra personuppgifter som man anser vara extra skyddsvärda (kan även kallas integritetskänsliga) men som inte omfattas av definitionen om känsliga personuppgifter.

Exempel på sådana uppgifter är:

- Personuppgifter som omfattas av sekretess eller tystnadsplikt (eller annan särlagstiftning, exempelvis Patientdatalagen)
- Personnummer
- Uppgifter och personliga och ekonomiska förhållanden
- Bild-, ljud- och videoinspelningar
- Omdömen och personlighetsbeskrivningar (preferenser, pålitlighet, beteenden mm.)

- Uppgifter om barn
- Uppgifter om lagöverträdelser

Datainspektionen har ställt krav på att starka säkerhetsåtgärder vidtas för det fall att sådana extra skyddsvärda personuppgifter på något sätt registreras så att de finns att nå via internet (öppna nät), exempelvis efter inloggning.

Exempelvis registreras det inom skolan en rad extra skyddsvärda uppgifter om barn, bland annat omdömen. Vidtagna säkerhetsåtgärder för registrering av dessa uppgifter gäller inte bara kommunikationen mellan skolan och elev/vårdnadshavare utan också om läraren de facto loggar in sig via internet för att registrera uppgifterna, exempelvis hemifrån.

1.5 Personuppgiftsansvarig

Varje nämnd är personuppgiftsansvarig för de behandlingar av personuppgifter som görs inom nämnden. Personuppgiftsansvarig är alltid en juridisk person, det går alltså inte att delegera personuppgiftsansvaret till en fysisk person. Ansvaret gentemot tillsynsmyndigheten och de registrerade ligger alltid kvar på den personuppgiftsansvarige, det vill säga nämnden, även när det gäller skadeståndsanspråk enligt GDPR.

Det är personuppgiftsansvariges skyldighet att vidta tekniska och organisatoriska åtgärder för att säkerställa att all behandling av personuppgifter följer GDPR och senare även den nya dataskyddsförordningen. Dataskyddsförordningen ställer också högre krav på att personuppgiftsansvarig ska kunna bevisa att man följer lagstiftningen genom att ha en förteckning, därför är det också viktigt att anmäla de verksamhetssystem som behandlar personuppgifter till personuppgiftsombudet (och senare dataskyddsombud).

1.6 Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för den personansvariges räkning. Personuppgiftsbiträdet finns alltid utanför den personuppgiftsansvariges organisation. Typiska biträdessituationer är till exempel när en IT-leverantör processar information i sina datorer för den personuppgiftsansvariges räkning genom att exempelvis trycka fakturor eller adresser. Det kan också vara företag som sköter passersystem eller en webbtjänst.

Observera att en biträdessituation inte endast behöver handla om lagring av personuppgifter, utan gäller även när en extern part har åtkomst till den personuppgiftsansvariges data genom sitt uppdrag för service, support, underhåll, utveckling och liknande. GDPR kräver att ett biträdesavtal upprättas mellan den personuppgiftsansvarige och personuppgiftsbiträdet. Du kan läsa mer om biträdesavtalet ovan.

I den nya dataskyddsförordningen blir även personuppgiftsbiträdet skyldig att föra en förteckning över sina personuppgiftsbehandlingar och vidta lämpliga

säkerhetsåtgärder. Personuppgiftsbiträdet kan även komma att bli föremål för tillsyn, administrativa sanktionsavgifter samt bli skadeståndsskyldiga.

1.7 Personuppgiftsombud

Ett personuppgiftsombud är en person som ser till att personuppgifter behandlas på ett korrekt och lagligt sätt inom den egna organisationen. Personuppgiftsombudet kan jämföras med en internrevisor som påpekar fel och brister till den som är personuppgiftsansvarig. När den personuppgiftsansvarige (nämnden) utsett ett personuppgiftsombud anmäls det till Datainspektionen.

I den nya dataskyddsförordningen ändras benämningen för personuppgiftsombud till dataskyddsombud. Ombudets roll är fortfarande att se till att personuppgifter behandlas på ett korrekt och lagligt sätt samt att vara organisationens kontaktperson gentemot tillsynsmyndigheten.

1.8 Helt eller delvis automatiserad behandling

Personuppgiftslagen tillämpas på all behandling av personuppgifter som utförs helt eller delvis med hjälp av datorer. Helt automatiserad behandling innebär att personuppgifter registreras direkt i exempelvis ett verksamhetssystem och behandlingen framöver fortsätter att ske digitalt.

Delvis automatiserad behandling innebär att personuppgifter samlas i manuellt, exempelvis genom en enkät, med syftet att senare registrera uppgifterna digitalt. Detsamma gäller om uppgifter som lagras digitalt skrivs ut på papper eller förmedlas vidare muntligt. Vid delvis automatiserad behandling är det viktigt att ha bra rutiner för förvaring och gallring, risken är annars att samma uppgifter sparas på fler platser än nödvändigt.

1.9 Manuella register

Manuell behandling av personuppgifter i register (till exempel ett klassiskt kartotek eller närarkiv) omfattas av personuppgiftslagen om uppgifterna är sorterade enligt något slags system som gör det möjligt att söka bland uppgifterna. En hög med papper på ett skrivbord anses inte vara ett register även om de är sorterade i bokstavsordning efter efternamn. För att det ska vara ett manuellt register som omfattas av personuppgiftslagen krävs att samlingen av personuppgifter är strukturerad i syfte att påtagligt underlätta eftersökning och sammanställning av personuppgifter.

Personuppgiftsansvarig: Den som ensam eller tillsammans med andra bestämmer ändamål med och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde: Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.

2 Introduktion

I kommunen hanterar vi en mängd personuppgifter. Det kan handla om personuppgifter om medarbetare, elever, enskilda som söker bygglov eller ekonomiskt bistånd och så vidare. När vi hanterar personuppgifter så behöver vi säkerställa att kommunens hantering är i enlighet med gällande lagstiftning. I denna guide får du som medarbetare information om vad som är viktigt att tänka på när du hanterar personuppgifter utifrån gällande lagstiftning.

Den 25 maj 2018 ersattes personuppgiftslagen (GDPR) av en ny dataskyddsförordning. Dataskyddsförordningen (även kallad GDPR) är ett regelverk för behandling av personuppgifter som har tagits fram av EU. Syftet med lagstiftningen är att skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas.

Denna riktlinje ska ses som ett levande dokument som kommer att uppdateras allt eftersom.

2.1 Först och främst ska det vara nödvändigt

För alla behandlingar av personuppgifter finns alltid ett krav på nödvändighet. De personuppgifter som samlas in ska vara nödvändiga för ändamålet och därför ska heller inga onödiga personuppgifter samlas in.

Tips! Ta för vana att ifrågasätta om alla de uppgifter som registreras faktiskt är nödvändiga för ändamålet. Det är sällan ett personnummer behövs på en deltagarlista till exempel. Samla inte in fler personuppgifter än vad som verkligen är nödvändigt.

2.2 Finns det en rättslig grund behövs inget samtycke

Vid följande situationer är det tillåtet att behandla personuppgifter utan samtycke:

- Avtalssituation – Behandling av personuppgifter är nödvändig för att uppfylla ett avtal mellan den personuppgiftsansvarige och den enskilde. Exempel: Behandlingar för administration av kundförhållande eller anställningsförhållande.
- Rättslig skyldighet - Behandling av personuppgifter har stöd av annan författning. Exempel: Lämna ut uppgifter om anställda till bland annat statliga myndigheter för att redovisa skatter och sociala avgifter beträffande arbetstagarna.
- Vitala intressen - Behandling av personuppgifter är tillåten om det sker för att skydda den registrerades vitala intressen som liv och hälsa. Exempel: Vanligt inom sjukvården. Detta är en ovanlig rättslig grund för kommunal verksamhet.
- Allmänt intresse - Gäller när behandling av personuppgifter är nödvändig för att utföra en uppgift av allmänt intresse. Exempel: Arkivering, forskning och framställning av statistik.
- Myndighetsutövning - Behandling av personuppgifter är tillåten om det är nödvändigt för myndighetsutövning. Med myndighetsutövning menas här sådana uppgifter som en myndighet enligt lag ska utföra och som har rättsliga effekter för den enskilde. Observera att detta inte innebär att alla personuppgiftsbehandlingar i en myndighet sker på denna grund, exempelvis är personaladministrativa åtgärder fortfarande en avtalssituation. Exempel: Ansökan om ekonomiskt bistånd eller bygglov.
- Intresseavvägning - Kan tillämpas när den personuppgiftsansvariges intresse att behandla en uppgift väger tyngre än den enskildes personliga integritet, när ändamålet för behandlingen rör ett berättigat intresse hos den personuppgiftsansvarige. OBS! En intresseavvägning blir inte längre tillämplig för myndigheter i den nya dataskyddsförordningen som börjar gälla den 25 maj 2018.

3 Personuppgifter i e-post

E-post som innehåller personuppgifter kan skickas så länge de inte innehåller:

- Känsliga personuppgifter, t.ex. hälsoinformation (se fler exempel i avsnittet ”Definitioner”).
- Extra skyddsvärda uppgifter, t.ex. sekretessbelagd information enligt offentlighets- och sekretesslagen eller personnummer (se fler exempel i avsnittet ”Definitioner”).

I dagsläget är inte kommunens e-post krypterad vilket innebär att vi inte ska skicka känsliga eller extra skyddsvärda personuppgifter via mejl. Om du avidentifierar innehållet så kan du däremot skicka uppgifterna, det förutsätter däremot att mottagaren också förstår vem information berör.

I de fall vi ändå behöver skicka e-post som innehåller känsliga personuppgifter eller sekretessbelagd information i sin helhet så krävs att särskilda säkerhetsåtgärder vidtas. Med säkerhetsåtgärder avses i praktiken krypteringsskydd på ett sådant sätt att endast den avsedda mottagaren kan ta del av dem. Vissa e-postsystem har funktioner för att kryptera meddelanden mellan användare inom samma e-postdomän men vanligtvis behövs särskilda krypteringsnycklar eller programvaror för att kryptera e-post.

3.1 Arbetar du inom hälso- och sjukvården?

Inom hälso- och sjukvården gäller särskilda bestämmelser utifrån Socialstyrelsens föreskrifter - Informationshantering och journalföring inom hälso- och sjukvården. Föreskrifterna innehåller bestämmelser om hantering av patientuppgifter över öppna nät som innebär att överföring av patientuppgifter ska göras på ett sådant sätt att ingen obehörig kan ta del av uppgifterna. Det gäller även för e-post och innebär i praktiken ett krav på att patientuppgifterna i ett e-postmeddelande ska krypteras på ett sådant sätt att endast den avsedda mottagaren kan ta del av dem.

3.2 Hur gör jag om någon skickar e-post till mig med känsliga personuppgifter eller sekretessuppgifter?

Om någon skickar känsliga personuppgifter eller sekretessuppgifter så innebär det inte att hen gett sitt samtycke till att hantera personuppgifter per e-post. Den enskilde har ingen information om huruvida kommunens e-post är krypterad eller ej och ett samtycke är därför inte aktuellt. Tänk därför på att du inte svarar genom att skicka med det innehåll som omfattas av sekretess. Dessa uppgifter måste tas bort i svarsmejlet.

4 Var försiktig med personnummer

Tvärt emot vad många tror, finns det inte något förbud mot att registrera personnummer eller samordningsnummer (samordningsnummer är ett unikt identifikationsnummer som kan tilldelas personer som inte är eller har varit folkbokförda i Sverige). Även om ett personnummer inte är en känslig personuppgift så betraktas den som extra skyddsvärd och därför får personnummer inte används hur som helst.

Överväg alltid om det är nödvändigt att notera personnummer på alla ställen som du har tänkt det, eller om det räcker med att det finns tillgängligt till exempel i en akt eller enbart i en grunddatabas. Det är framförallt den slentrianmässiga användningen av personnummer som man måste vara observant på, exempelvis i mejlkonversationer. Tänk efter; stödjer syftet med behandlingen av personuppgifter att personnummer registreras?

Personnummer ska enbart användas:

- om den registrerade har samtyckt till registreringen,
- om behandlingen är klart motiverat med hänsyn till ändamålet med behandlingen (räcker det med förslagsvis namn och adress, födelsedatum eller födelseår, så ska du nöja dig med det),
- om behandlingen är klart motiverat med hänsyn till vikten av en säker identifiering. Exempelvis är det tillåtet att registrera de anställdas personnummer i ett register som innehåller grunddata eller till exempel ett löneadministrativt IT-system, för redovisning av källskatter, vid rehabiliteringsutredning eller kommunikation med facket i lönerevisioner, i ett kommuninvånarregister och elevers personnummer i ett skoladministrativt IT-system. Personnummer behövs i dessa fall på grund av vikten av en säker identifiering, det vill säga man måste vara säker på vem personen är när man exempelvis sätter betyg, administrerar ansökningar till barnomsorg eller äldreomsorg, i tillsynsärenden på miljöenhet, i kravärenden och när kommunen rapporterar till skatteverket.
- om behandlingen är klart motiverat med hänsyn till något annat beaktansvärt skäl.

Bestämmelserna om personnummer gäller däremot inte födelsedatum. Datainspektionen har ändå ansett att det är tveksamt om det finns anledning att registrera födelsedatum på till exempel en deltagarlista. Är det inte viktigt när någon fyller år eller hur gammal han eller hon är, behövs ju varken födelsedatum eller födelseår.

Vill du motivera din registrering av personnummer med att den är tillåten på grund av vikten av en säker identifiering ska du göra en slags intresseavvägning. Vid en sådan avvägning ska resultatet bli att det är viktigare att det inte sker något misstag i identifieringen av den registrerade (förväxling av person), än vad det är att skydda den registrerades personliga integritet. Du kan läsa mer om intresseavvägning i 10§ f GDPR.

4.1 Personnummer som användaridentitet

Undvik att använda personnummer som användaridentitet vid inloggningar. I stora organisationer med många anställda har Datainspektionen i undantagsfall godtagit användning av personnummer både för behörighetsadministration och inloggning om det behövs för en säker identifikation av användaren. Om det finns behov av att använda personnummer som inloggning så behövs samråd med kommunens personuppgiftsombud/dataskyddsombud.

5 Avidentifierade eller krypterade personuppgifter

Om informationen du har registrerad de facto är avidentifierad så rör det sig inte längre om en behandling av personuppgifter och bestämmelserna i GDPR blir inte tillämpliga. För att personuppgifterna ska anses vara avidentifierade så krävs dock att man inte kan hitta tillbaka till en enskild individ även om man tillför annan information, till exempel en krypteringsnyckel. Det har ingen betydelse om krypteringsnyckel är inbyggd i ett verksamhetssystem eller om den är nedskriven på ett papper, så länge den finns att tillgå så är inte personuppgifterna avidentifierade. Inom statistik och forskning är användningen av avidentifierade uppgifter vanligt då svar och resultat inte går att härleda till en enskild individ.

Kryptering är en teknisk säkerhetsåtgärd men innebär alltså inte att informationen är avidentifierad och därför är GDPR tillämplig på även krypterade uppgifter. I Datainspektionens vägledning kring informationssäkerhet fastställs att känsliga personuppgifter ska vara krypterade vid överföring, exempelvis i mejlkommunikation.

6 Hanterar ett externt företag personuppgifter för kommunens räkning?

Det är vanligt att ett externt företag, som till exempel systemleverantör, support eller utförare, behandlar personuppgifter åt nämnden. Den externa parten kallas då personuppgiftsbiträde. Biträdet finns alltid utanför den personuppgiftsansvariges egen organisation. Personuppgiftsbiträdet behöver inte lagra personuppgifterna utan det räcker att den externa parten har tillgång till den personuppgiftsansvariges data för att räknas som ett personuppgiftsbiträde.

6.1 Ta fram ett personuppgiftsbiträdesavtal

I alla biträdessituationer ska det finnas ett skriftligt avtal (personuppgiftsbiträdesavtal) mellan den personuppgiftsansvarige och biträdet. I ett sådant avtal villkoras biträdets hantering av personuppgifterna och det är den personuppgiftsansvarige som är skyldig att se till att skriftliga biträdesavtal finns. Det är oftast enklast och tydligast att ha biträdesavtalet som en del av tjänsteavtalet. Då slipper man göra en separat beskrivning av uppdraget, som kanske senare ändras i tjänsteavtalet utan att någon tänker på att även biträdesavtalet måste ändras på samma sätt.

På kommunens hemsida hittar du information om vilka lagkrav som ställs på innehållet i biträdesavtalet. Kravlistan är framtagen utifrån den nya dataskyddsförordningen.

7 Publicering av personuppgifter på hemsidan

Personuppgifter om enskilda får endast publiceras på hemsidan om det finns rättslig grund för det. Tänk på att personuppgifter som enskilt kan betraktas som harmlösa kan anses som vara kränkande beroende på sammanhanget de publiceras i. Känsliga eller extra skyddsvärda personuppgifter får aldrig publiceras på webben.

7.1 Samtycke är alltid ett bra alternativ för publicering

Är du osäker på om en uppgift kan anses vara integritetskränkande så använd dig av möjlighet att hämta in samtycke. Samtycker den enskilde så kan du publicera uppgifterna. Fyller den enskilde i en ansökan digitalt eller i pappersformat så kan du alltid be om samtycke i samband med ansökan. Viktigt är att alla samtycken, oavsett hur de inhämtas, dokumenteras för att kunna hänvisa till dessa. Läs mer om samtycke i senare avsnitt.

7.2 Offentlighetsprincipen då?

Offentlighetsprincipen och integritetsskyddslagstiftningen (GDPR) har olika syften. Enbart det faktum att en handling är allmän och offentlig innebär inte att det är tillåtet att publicera den på hemsidan. Enligt offentlighetsprincipen finns det heller ingen skyldighet att publicera information på internet. Det innebär i sin tur att personuppgiftslagens regler måste följas när det kommer till webbpublicering. Det kan illustreras med nedan exempel:

En nämnd beslutar om att vitesförelägga en privatperson för brott mot miljöbalken.

Hur ska beslutet hanteras utifrån:

- Offentlighetsprincipen?
  - × Om någon begär att få ta del av beslutet så är det en offentlig handling och ska lämnas ut.
- Personuppgiftslagen?
- Eftersom handlingen innehåller information om lagöverträdelser ska handlingen inte publiceras på hemsidan.

7.2.1 Webbdiarium

Att publicera diarier och protokoll på hemsidan sker inte med stöd av offentlighetsprincipen utan går utöver kommunens skyldighet enligt grundlagen – med det sagt är det heller inte otillåtet att ha ett webbdiarium. För de handlingar som publiceras i webbdiariet gäller däremot GDPR.

Personuppgifter som direkt pekar ut en enskild får inte publiceras i webbdiariet, undantaget förtroendevalda i deras roll som förtroendevalda och tjänstemän i deras roll som tjänstemän. Direkt utpekande uppgifter är exempelvis namn och personnummer, indirekta uppgifter är exempelvis fastighetsbeteckning. Det är dock enskilda uppgifter i handlingarna som ska döljas, inte hela diarieposten i sig.

Obs! Känsliga personuppgifter får under inga omständigheter publiceras på hemsidan. Tänk på att bara uppgiften om att en enskild förekommer i ett ärende kan vara en känslig personuppgift.

7.3 Särskilt om fotografering

Att publicera foton på anställda på hemsidan kräver i regel samtycke från den anställde. Det finns dock undantag där en intresseavvägning gör det tillåtet att publicera foton (exempelvis porträttfoton i kombination med namn och eventuella kontaktuppgifter). Undantaget gäller bland annat hemtjänstpersonal, fastighetsskötare eller liknande för att kunden ska veta att den släpper in rätt person i sitt hem. Även personer i ledande ställning, som tjänstemannaledningen, kan räkna med att få sin bild publicerad på hemsidan.

Inom skola, förskola och fritids måste vårdnadshavare samtycka innan en publicering av barn sker på hemsidan. Samtycket ska inhämtas från båda vårdnadshavarna. Om samtycket utformas på ett korrekt sätt behöver det bara inhämtas en gång för alla bilder som publiceras under hela skoltiden. Kontakta personuppgiftsombudet för att få hjälp med att ta fram en samtyckesblankett för dina ändamål.

Tänk på att det kan finnas enskilda med skyddade personuppgifter i skolan. Läs mer om hur du hanterar skyddad identitet i senare avsnitt.

7.4 Särskilt om sociala medier

När Torsby kommun som organisation publicerar personuppgifter i sociala medier (Facebook, Twitter, Instagram, Youtube m.fl.) så finns ett personuppgiftsansvar. I personuppgiftsansvaret ingår att:

- inte publicera kränkande personuppgifter,
- hålla regelbunden uppsikt över publiceringar för att upptäcka kränkande personuppgifter,
- skyndsamt ska ta bort kränkande personuppgifter,
- vidta lämpliga säkerhetsåtgärder (det innebär bland annat att kommunen ska ge instruktioner till de som arbetar med sociala medier för organisationens räkning, anställda och andra som agerar på uppdrag av kommunen).

Läs mer om kommunens riktlinjer för sociala medier här ->

I personuppgiftsansvaret ingår det alltså att se till att det hålls en god ton bland besökarna på till exempel kommunens Facebook-sida. För att minska risken för kränkningar av enskildas personliga integritet menar Datainspektionen att den

personuppgiftsansvarige också bör vidta åtgärder i förebyggande syfte. Det kan till exempel vara att:

- informera om för vilka ändamål som kommentarsfunktionen är tänkt att användas, vilka typer av kommentarer som inte får förekomma och att publiceringar kan komma att plockas bort,
- uppmana användare att rapportera kränkande innehåll till organisationen och ha rutiner för att hantera klagomål.

8 Gallra personuppgifter

Kortfattat kan det sägas att det är ändamålet, alltså anledningen till att personuppgifterna behandlas, som avgör hur länge uppgifterna får sparas innan de gallras. Ändamålet för behandlingen måste bestämmas redan innan personuppgifterna samlas in och registreras. Ändamålet ska kunna anges uttryckligen. Gallring av personuppgifter ska föregås av ett beslut. Regler om gallring hindrar dock inte att en myndighet (nämnden), arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Bestämmelserna om allmänna handlingar enligt offentlighets- och sekretesslagen har då företräde framför bestämmelserna i GDPR.

8.1 Hur tar man bort personuppgifter?

Det finns två olika sätt att ta bort personuppgifter. Man kan antingen avidentifiera eller förstöra (gallra) dem:

- Avidentifiera
- Att avidentifiera personuppgifterna innebär att man avlägsnar alla identifieringsmöjligheter så att de uppgifter som fortsättningsvis behandlas inte längre går att koppla samman med en fysisk person. Krypterade personuppgifter är inte avidentifierade så länge någon kan göra uppgifterna läsbara och därmed identifiera personen.
- Förstöra (gallra)
- Att förstöra personuppgifterna innebär att se till att de inte går att återskapa. Det är viktigt att känna till vad som krävs rent tekniskt för att uppgifterna verkligen ska förstöras. Det är till exempel inte tillräckligt att radera den fil som innehåller personuppgifterna. Det är nämligen inte säkert att ett sådant kommando verkligen raderar all information, filen kan exempelvis ligga kvar i datorns "papperskorg". I stället krävs säker omformatering av lagringsmediet eller total överskrivning så att personuppgifterna inte kan tolkas i efterhand. Det är däremot inte heller säkert att vanlig formatering raderar alla uppgifter utan det kan krävas särskild utrustning eller specialprogramvaror. Hur långtgående tekniska åtgärder som bör vidtas är bland annat beroende av informationens känslighet.

Exempel 1: Är ändamålet bara att kunna veta vilka personer som finns i huset och var, vid en eventuell evakuering, är gallringstiderna förstås väldigt korta. Ändamål som att känna igen personens namn nästa gång hen kommer, och föreslå mottagarnamn,

kräver normalt samtycke, vilket kan vara lite krångligt att administrera. Tänk på att lämna kort information om registreringen enligt 23–25 §§ GDPR till exempel på startsidan (det görs väldigt sällan i besökssystem men är egentligen ett krav).

Exempel 2: Personuppgifter som inkommer i en rekryteringsprocess (ansökan, intervjuanteckningar och uppgifter referenser) bör normalt gallras bort när anställningsförfarandet har avslutats. Arbetsgivaren får däremot uppgifterna så länge den sökande till exempel har möjlighet att överklaga beslutet om att denne inte fick jobbet. Vill arbetsgivaren använda uppgifterna längre, till exempel för framtida rekrytering, måste den arbetssökande informeras och samtycka till fortsatt registrering. För uppgifter om den som blivit anställd gäller andra gallringsfrister.

8.2 Dokumenthanteringsplanen anger när det ska gallras

Är du osäker på när en handling ska gallras (och tillhörande personuppgifter) så anges gallringsfristen i den dokumenthanteringsplan som varje nämnd antagit. Ingen handling får gallras utan ett att beslut har fastställts i en dokumenthanteringsplan.

Dokumenthanteringsplanen gäller både för digitala handlingar och fysiska handlingar. Av dokumenthanteringsplanen framgår även om speciallagstiftning anger särskild gallringsfrist (till exempel patientdatalagen).

9 Varje behandling av personuppgifter ska anmälas till personuppgiftsombudet

Behandlingar av personuppgifter ska anmälas till kommunens personuppgiftsombud. I princip innebär det att all helt eller delvis automatiserad behandling av personuppgifter ska anmälas till ombudet. Vanligtvis rör det sig om behandling av personuppgifter i digitala verksamhetssystem, men även manuella register i exempelvis pärmar eller annan strukturerad samling av personuppgifter ska anmälas.

Förteckningen är en förutsättning för att kommunen ska kunna fullgöra sin skyldighet att lämna registerutdrag till den som efterfrågar det. Förteckningen ger också viktig information över hur dataflödena ser ut inom kommunen och hur kommunen efterlever lagstiftningen. Det är därför av stor vikt att alla nya behandlingar anmäls till personuppgiftsombudet.

9.1 Hur anmäler jag en behandling?

Du anmäler en personuppgiftsbehandling genom att besvara ett webbaserat formulär. För att få tillgång till formuläret måste du kontakta personuppgiftsombudet som ser till att du får en länk skickad till dig. Följ länken och besvara frågorna. Spara gärna länken eftersom du då lätt kan gå tillbaka till formuläret och ändra eller uppdatera information. Om du tappar bort länken så kontakta personuppgiftsombudet för hjälp.

Genom att anmäla behandlingen i god tid innan behandlingen sätts igång har du tid att säkra att behandlingen sker i enlighet med GDPR. Det är ofta i samband med anmälan som det är lätt att upptäcka om det finns brister när det gäller hanteringen. Kanske behöver säkerheten för personuppgifterna ses över ytterligare eller ett

samtycke inhämtas med den enskilde. När det gäller känsliga personuppgifter så kan en särskild konsekvensbedömning behöva genomföras innan behandlingen påbörjas.

10 Vilka säkerhetskrav ska ställas på en personuppgiftsbehandling?

För alla som hanterar och bearbetar personuppgifter är det viktigt att säkerställa att personuppgifterna skyddas på ett bra sätt. Den personuppgiftsansvarige måste vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna. Tekniska åtgärder omfattar saker som brandväggar, krypteringsfunktioner och anti-virus, medan organisatoriska åtgärder handlar om säkerhetsarbetets organisation, rutiner och styrdokument. Behandling av känsliga och extra skyddsvärda personuppgifter ställer högre krav på vidtagna säkerhetsåtgärder.

Följande frågeställningar kan vara till hjälp när man bedömer hur pass känsliga uppgifterna är:

- Omfattas uppgifterna av tystnadsplikt eller sekretess enligt offentlighets- och sekretesslagen eller annan lagstiftning?
- Omfattas behandlingen av någon särlagstiftning, till exempel patientdatalagen eller lagen om behandling av personuppgifter inom socialtjänsten med flera?
- Är det uppgifter om lagöverträdelser?
- Är det uppgifter om enskildas personliga förhållanden?

Är svaret Ja på någon av dessa frågor ska säkerhetsåtgärderna för att skydda personuppgifterna vara mer omfattande.

10.1 Konsekvensbedömning

Att genomföra en konsekvensbedömning för en särskild personuppgiftsbehandling är en bra utgångspunkt för att säkerställa en säker och korrekt behandling. I konsekvensbedömningen tar den personuppgiftsansvarige ställning till lämpliga säkerhetsåtgärder, risker och konsekvenser samt bedömer hur känsliga de behandlade uppgifterna är.

Frågor som ställs i en konsekvensbedömning:

- Behandlas personuppgifterna på ett sätt som gör det svårt att kontrollera att det bara sker i enlighet med ändamålen med behandlingen? Finns det risk för att personuppgifterna kan spridas på ett oönskat sätt?
- Hanteras personuppgifter via öppna nät som internet, till exempel via en webbsida eller genom e-post?
- Kan många användare komma åt personuppgifterna?
- Behandlas personuppgifter om många personer?
- Behandlas en stor mängd personuppgifter om varje person?

- Hur stor är sannolikheten för och konsekvenserna av tekniska störningar eller att obehöriga får åtkomst till uppgifterna?

Ju fler av dessa frågor som man svarar Ja på desto mer omfattande bör säkerhetsåtgärderna vara. Åtgärder som vidtas ska bidra till en adekvat säkerhetsnivå som är lämplig i förhållande till tillgänglig teknik, kostnader, de särskilda riskerna med behandlingen och hur pass känsliga uppgifterna är.

I den nya dataskyddsförordningen har den personuppgiftsansvarige en skyldighet att genomföra en konsekvensbedömning, en typ av risk- och sårbarhetsanalys, för varje ny behandling av känsliga personuppgifter. Konsekvensbedömningen är ett effektivt hjälpmedel för den personuppgiftsansvarige att säkerställa en korrekt och säker behandling av personuppgifter. Mall för konsekvensbedömning finns på kommunens hemsida och du kan också få stöd i genomförandet. Tänk på att dokumentera resultatet från konsekvensbedömningen.

10.2 Att arbeta på distans – tänk på det här

När du arbetar på distans är det extra viktigt att du tänker på hur du behandlar eventuella personuppgifter i ditt arbetsmaterial. All verksamhetsrelaterad information ska lagras på gemensamt diskutrymme (Q:). I skydd av åtkomstbegränsning och med utökad spårbarhet kan även känslig eller sekretessbelagd information lagras på samma plats. Använd alltså inga andra lagringsytor för ditt arbetsmaterial (till exempel Dropbox, Google drive eller liknande). Använd inte heller din privata e-postadress för att kommunicera med kollegor om personuppgifter om enskilda finns med i konversationen.

Begränsningen av hur och var arbetsrelaterad information, inklusive personuppgifter, lagras är en del av Torsbys informationssäkerhetspolicy. Du kan läsa mer om policyn samt ta del av stöd och riktlinjer här genom att följa denna länk:

11 Skyddade/sekretessmarkerade personuppgifter

Om någon är utsatt för ett allvarligt hot kan Skatteverket besluta om skyddade personuppgifter i särskilda fall. Det finns tre typer av skyddade personuppgifter: sekretessmarkering, kvarskrivning och fingerade personuppgifter.

När det gäller behandling av skyddade personuppgifter ska den personuppgiftsansvarige, utöver att se till att behandlingen följer GDPR, även tänka på följande:

- Regler och rutiner ska finnas för att säkerställa att skydda personuppgifter behandlas på ett sådant sätt att det inte innebär en ökad risk för registrerade.
- En riskbedömning ska göras från fall till fall då behovet av vilka uppgifter som behöver särskilt skydd varierar.

- Vid behandling av skyddade personuppgifter är det extra viktigt att endast registrera uppgifter nödvändiga för ändamålet, dessa ska även gallras så snart de inte längre behövs.
- Den personuppgiftsansvarige bör begränsa åtkomsten till de skyddade personuppgifterna till ett fåtal personer. För de personer som har åtkomst till uppgifterna ska det också tydligt framgå att de är skyddade (exempelvis genom flaggning).
- Den personuppgiftsansvarige bör se till att skyddade personuppgifter inte okontrollerat sprids mellan olika verksamhetssystem som utbyter data. Det är alltså viktigt att skyddade personuppgifter inte sprids till ett system med sämre säkerhet. Den personuppgiftsansvarige är skyldig att vidta lämpliga säkerhetsåtgärder (med hänsyn till den konsekvensbedömning som gjorts avseende behandlingen).
- All personal som kommer i kontakt med skyddade personuppgifter måste få kunskap om de regler och rutiner som gäller.
- Se till att verksamhetssystem som behandlar skyddade personuppgifter genererar loggar så att det i efterhand går att kontrollera vem som har haft tillgång till informationen. Glöm inte att följa upp och kontrollera loggarna!

12 Registerutdrag

Alla har rätt att vända sig till kommunen och begära att få veta vad som finns registrerat om hen. Det kallas att man begär ett registerutdrag. Ett registerutdrag innebär att organisationen ska lämna information om vad som finns registrerat i IT-systemen om en specifik person. Utdraget får bara gälla den person som har begärt det, självklart kan ingen begära ett registerutdrag gällande någon annan person (det finns vissa undantag avseende förvaltare, gode män och vårdnadshavare).

Var och en som är registrerad har rätt till ett kostnadsfritt utdrag per år. Det finns alltså ingen möjlighet att ta betalt för kostnader i samband med att registerutdraget tas fram. När som helst kan det inkomma en begäran om registerutdrag till kommunen. Det är den personuppgiftsansvarige som ansvarar för att registerutdraget är korrekt och lämnas i tid och det görs under straffansvar.

Blanda inte ihop skyldigheten enligt GDPR att lämna registerutdrag, med skyldigheten enligt offentlighetsprincipen att lämna ut allmänna och offentliga handlingar. En handling behöver inte vara vare sig offentlig eller allmän för att den ska ingå i ett registerutdrag. Registerutdragen som lämnas blir däremot alltid allmänna handlingar, som kan vara offentliga eller omfattas av sekretess enligt de vanliga reglerna om offentlighet och sekretess.

Så länge GDPR gäller är den personuppgiftsansvarige endast skyldig att tillmötesgå en skriftlig begäran om registerutdrag. Men i den nya dataskyddsförordningen är det även möjligt att begära ett registerutdrag elektroniskt och då ska det även vara möjligt att få den informationen i ett elektroniskt format. Exakt hur det ska gå till att lämna registerutdrag (och även allmänna handlingar som innehåller personuppgifter) elektroniskt via nätet är ännu inte klarlagt.

12.1 Säkerställ att registerutdraget skickas till rätt person

En begäran om registerutdrag ska vara skriftlig och egenhändigt undertecknad av den som utdraget avser. Det duger alltså inte med en fullmakt. Lämna inte ut ett registerutdrag om en begäran kommit in per e-post eller muntligen, om du inte är säker på att du lämnar ut till rätt person. Skicka alltid registerutdrag till folkbokföringsadress och innehåller registerutdraget känsliga personuppgifter så bör försändelsen dessutom skickas som REK.

12.2 Inom rätt tid

Försök att lämna registerutdraget i tid, allra helst inom en månad. Det finns dock möjlighet att vänta upp till fyra månader innan utdraget lämnas, men då ska det föreligga särskilda skäl och den som begär utdraget ska informeras om förseningen och orsaken till den. Det ska då vara sakliga skäl för förseningen. Som sakliga skäl räknas inte semester, arbetsanhopning eller att det råder osäkerhet vart personuppgifterna kan finnas registrerade någonstans.

Registerutdraget behöver dock inte innehålla personuppgifter från löpande text som inte fått sin slutgiltiga utformning (arbetsmaterial) när den registrerade gjorde sin ansökan eller personuppgifter från minnesanteckningar. Detta eftersom personuppgifterna inte är sökbara och Datainspektionen menar att det inte heller skulle gagna den enskildes integritet att göra identitetsuppgifter i sådant material sökbara.

Är du osäker på hur du ska hantera en begäran om registerutdrag kan du vända dig till personuppgiftsombudet.

Vad ska ingå i registerutdraget?

- Ett utdrag med alla de personuppgifter som rör den personen som sökt
- Var uppgifterna har hämtats
- Vad uppgifterna används till
- Till vilka mottagare (eller kategorier av mottagare) som uppgifterna har lämnats ut

13 Informationsplikt

Enligt GDPR har den personuppgiftsansvarige informationsplikt gentemot de registrerade. De personer som har sina personuppgifter registrerade ska alltså få information om detta. Information lämnas lämpligen i samband med att personuppgifterna hämtas in och på samma medium, alltså muntligt vid samtal, skriftligt på en blankett eller på hemsidan om den registrerade lämnar sina personuppgifter på webben. I den nya dataskyddsförordningen kommer det att ställas högre krav på att den information som lämnas är lättbegriplig och tydlig – detta för att de registrerade lättare ska kunna utöva sina rättigheter att exempelvis begära rättelse av uppgifter. På Torsbys hemsida finns exempel på hur informationstexten kan utformas.

Informationen som lämnas ska innehålla:

- kontaktuppgifter till den personuppgiftsansvarige • den rättsliga grunden för behandlingen
- ändamålet med behandlingen.
- information om personuppgifterna kan komma att lämnas ut till tredje part och i så fall för vilka syften
- rätten att begära registerutdrag
- rätten att få sina personuppgifter rättade vid felaktigheter eller raderade
- Hur länge personuppgifterna kommer att lagras

Om redan insamlade personuppgifter kommer att användas för ett annat syfte (ändamål) än för vilket de samlades in måste ny information lämnas till de registrerade – det vill säga information om ändamålet för den nya behandlingen. Information måste även lämnas vid händelse av dataintrång om det finns risk för exempelvis bedrägeri eller identitetsstöld (incidentrapportering).

14 Samtycke till behandling av personuppgifter

Samtycke innebär att den registrerade har gett sitt godkännande till att få sina personuppgifter behandlade. I GDPR är utgångspunkten att personuppgiftsbehandling endast är tillåten när den registrerade har lämnat sitt samtycke, om inte annan rättslig grund för behandling finns. Samtidigt ställs det också krav på att information lämnas till de registrerade (läs mer i avsnittet ovan). Läs mer om rättslig grund i tidigare avsnitt.

Ett samtycke ska vara individuellt, frivilligt och särskilt. Ett samtycke kan därför inte lämnas för någon annans räkning och den registrerade ska också ha möjlighet att själv avgöra om personuppgifterna ska få behandlas. Ett lämnat samtycke gäller också för ett enda ändamål, om de insamlade personuppgifterna ska användas för ett annat ändamål än för vilket de samlades in krävs ett nytt samtycke för det nya ändamålet.

För behandling av känsliga personuppgifter ställs det högre krav på att samtycket är uttryckligt, alltså att det är extra tydligt. Ett konkludent samtycke där uppgiftslämnandet i sig utgör ett samtycke är inte godtagbart för registrering av känsliga personuppgifter.

I GDPR ställs det däremot inga krav på att samtycket ska vara skriftligt, men det är en god idé att dokumentera inhämtade samtycken eftersom det är den personuppgiftsansvarige som har bevisbördan i de fall ett samtycke ifrågasätts.

Kontakta personuppgiftsombudet för hjälp att ta fram en samtyckesblankett för dina ändamål.

14.1 Återkalla samtycke

I de fall en personuppgiftsbehandling utförs endast med stöd av samtycke från den registrerade så kan samtycket också återkallas. Ett återkallat samtycke innebär att den personuppgiftsansvarige inte får registrera nya uppgifter om den enskilde. Den personuppgiftsansvarige får däremot fortsätta att behandla redan insamlade personuppgifter men de får inte uppdateras eller ändras, risken att dessa också blir rent av felaktiga är därför stor.

15 E-tjänster och personuppgifter

Alla e-tjänster behandlar i någon utsträckning personuppgifter (namn, adress, telefonnummer osv.). Det innebär att GDPR är tillämplig på behandlingen. Om e-tjänsten även behandlar känsliga personuppgifter krävs extra säkerhetsåtgärder. Valet av autentiseringsmetod bör utgå från känsligheten hos de personuppgifter som behandlas, mängden uppgifter och de risker som är förknippade med behandlingen (se avsnittet om säkerhetskrav ovan).

15.1 Generellt för alla e-tjänster

15.1.1 Information

I anslutning till e-tjänsten ska det lämnas information till användarna om behandlingen av personuppgifter. Det gäller oavsett om uppgifterna samlas in med eller utan de registrerades samtycke. Informationen ska upplysa om vem som är personuppgiftsansvarig, ändamålen med behandlingen, vilka som är mottagare av uppgifterna, eventuell skyldighet för den enskilde att lämna uppgifter och rätten att ansöka om registerutdrag och få felaktiga uppgifter rättade. Normalt kan informationen lämnas i en särskild ruta eller i ett särskilt fönster på webbplatsen i anslutning till e-tjänsten. Detta gäller även för webbaserade enkäter i exempelvis Proofx-verktyget.

15.1.2 Personuppgiftsbiträdeavtal

Om en utomstående leverantör behandlar personuppgifter för nämndens räkning, till exempel om de lagras på en server hos leverantören, blir denne ett personuppgiftsbiträde. Nämnden måste då i egenskap av personuppgiftsansvarig

upprätta ett skriftligt avtal – ett så kallat biträdesavtal – med leverantören. I avtalet ska det föreskrivas att leverantören får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att leverantören är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda uppgifterna.

15.1.3 Anmäla behandlingen till personuppgiftsombud

Behandling av personuppgifter ska anmälas till kommunens personuppgiftsombud som har en förteckning över alla behandlingar. Behandlas känsliga personuppgifter i e-tjänsten ska en dokumenterad konsekvensbedömning bifogas vid anmälan.

15.2 Allmänna handlingar

Tänk på att inkommande och utgående handlingar i en e-tjänst utgör allmänna handlingar utifrån bestämmelserna i offentlighets- och sekretesslagen. Det innebär att daglig diarieföring ska ske vilket omfattar även inkommande och utgående handlingar i e-tjänster.

15.3 Bedöm hur känsliga uppgifterna är

Enligt GDPR gäller särskilda begränsningar för behandling av vissa kategorier av personuppgifter. Uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen, uppgifter om lagöverträdelser samt uppgifter om enskilds personliga förhållanden (extra skyddsvärda eller extra skyddsvärda uppgifter) ska också behandlas på samma sätt som känsliga personuppgifter.

Särskilda krav som ställs på e-tjänst som behandlar känsliga personuppgifter (inklusive extra skyddsvärda uppgifter):

- Användaren av e-tjänsten måste kunna förvissa sig om att det är den personuppgiftsansvarige (nämnden) som är mottagare av uppgifterna. Detta kan lösas genom att till exempel använda ett signerat servercertifikat och SSL/TLS.
- Personuppgifter måste skyddas så att obehöriga inte kan ta del av dem genom exempelvis kryptering och servercertifikat
- Det krävs fungerande rutiner för behörighetstilldelning och tydliga riktlinjer för när det är tillåtet för personalen att ta del av personuppgifter, här kan utbildningsinsatser vara nödvändiga.
- Det ska finnas en behandlingshistorik (logg) som löpande registrerar användaridentitet, tidpunkt och vilka personuppgifter som användaren har haft åtkomst till eller bearbetat.

16 Guide falsk e-post / bluffmejl

Det förekommer frekvent att användare i Torsby får falsk e-post / bluff mejl. Avsändare kan se ut att vara en Torsby adress, från någon annan kommun, eller någon annan som verkar pålitlig för mottagaren. Torsby kommun arbetar inte med denna typ av utskick för att samla in information.

Var därför försiktig med att öppna e-postmeddelanden, klicka på länkar och öppna bifogade dokument när du inte är helt säker på vem avsändaren är.

Om du misstänker att din dator blivit smittad eller du delgivit lösenord till någon annan kontakta Helpdesk omgående.

16.1 Hur skyddar jag mig?

- Var försiktig med e-post från avsändare du inte känner.
- Var uppmärksam när du öppnar bifogade filer i e-post även från människor du känner. Ställ dig frågan om det verkar rimligt att denna person skickat en bilaga eller skulle skicka denna typ av information?
- Klicka inte på länkar i mejl utan att först kontrollera vilken adress det faktiskt går till Tips: ta för vana att själv skriva in adressen i sidan du ska till direkt i adressfältet då är det lättare att uppmärksamma om något inte verkar stämma.
- Om du misstänker att du fått falsk e-post ska du under inga omständigheter klicka på länken eller skriva i några uppgifter.
- Har du redan klickat på länken och börjat fylla i, stäng sidan du hamnat på med hjälp av krysset i övre högra hörnet, använd inte någon knapp på sidan märkt med t.ex. ”Avbryt” (dessa kan vara länkade till att informationen ändå sparas).
- Om du i övrigt är osäker hur på du skall agera, kontakta alltid med Helpdesk.

16.2 Mer om falsk e-post / bluffmejl

Bluffmejl / nätfiske är e-post som skickas från någon som utger sig för att vara någon annan (till exempel en kommun eller myndighet) och försöker komma åt personliga uppgifter så som lösenord, kortnummer och koder alternativt försöker de få mottagaren att klicka på en länk som innehåller skadlig kod. Skadlig kod kan vara t.ex. ett virus eller ett sk. randsomeware som låser dina data (i värsta fall flera datorer) och sen kräver en lösensumma för att ta bort låsningen.

Ofta innehåller mejlet information om att ett konto eller kort riskerar att stängas eller att det föreligger någon form av risk om länken inte klickas på / information inte lämnas.

Mottagaren uppmanas att registrera uppgifter eller säkerställa att allting är okej via en länk.