IMY. Integritetsskydds myndigheten

Vägledning till politiska aktörer om dataskyddsreglerna i samband med valkampanjer

Innehåll

1 Inledning 3
2 Checklista 4
3 När gäller dataskyddsförordningen (GDPR)? 5
3.1 Undantag med hänsyn till yttrande- och informationsfriheten 5
3.1.1 Förhållandet till tryckfrihetsförordningen och yttrandefrihetsgrundlagen 5
3.1.2 Undantag för journalistiska ändamål när TF och YGL inte är tillämpliga 6
4 När dataskyddsförordningen gäller 7
4.1 De grundläggande principerna 8
4.2 Rättslig grund 11
4.2.1 Samtycke 11
4.2.2 Intresseavvägning 13
4.3 Behandlingar som utförs på uppdrag av andra och gemensamt ansvar 16
4.4 Känsliga personuppgifter 18
4.4.1 Vad som kan vara känsliga uppgifter 18
4.4.2 Vilka undantag som gör behandling av känsliga personuppgifter tillåten 19
4.5 Rätt till information och utövande av rättigheter 21
4.6 Konsekvensbedömning kan krävas 22
4.7 Överföring till tredjeland 23
5 Rättsinformation 23

1 Inledning

Inför de allmänna valen bedrivs valkampanjer för att sprida information med de politiska partiernas budskap i syfte att påverka hur väljarna röstar. I samband med detta kan personuppgifter komma att behandlas på olika sätt:

- som en del av själva budskapen (t.ex. ”AA:s politik är bättre än BB:s”)
- vid urval av mottagare ur olika register
- när budskapen förmedlas i fysisk form (till exempel via post)
- när budskapen förmedlas genom elektroniska kanaler
- när skräddarsydda budskap riktas till en person eller grupp genom beteendestyrd annonsering på internet och i sociala medier som används för att öka budskapets spridning, räckvidd eller synlighet utifrån särskilda egenskaper och profilering av mottagarna (nedan ”inriktnings- och förstärkningstekniker”).

I många av dessa situationer är bestämmelserna i dataskyddsförordningen tillämpliga.

Inriktnings- och förstärkningstekniker som används för att sprida budskap på internet kan baseras på avancerad profilering och omfattande behandling av mottagarnas personuppgifter. Denna profilering kan bygga på slutsatser om enskildas intressen eller andra egenskaper som de inte aktivt själva har lämnat ut. Om sådana tekniker används i samband med valkampanjer kan det innebära risker för:

- otillbörlig påverkan på väljarna, särskilt om det inte sker på ett öppet sätt
- att personuppgiftsbehandlingen strider mot eller går utöver väljarnas rimliga förväntningar och därmed bryter mot de grundläggande principerna i dataskyddsförordningen om korrekthet och öppenhet
- att enskildas möjlighet att utöva kontroll över sina personuppgifter och sina rättigheter enligt dataskyddsförordningen försvåras
- hot mot den personliga integriteten och väljarnas grundläggande fri- och rättigheter
- hot mot den demokratiska processen (se till exempel den så kallade Cambridge Analytica-skandalen (extern länk) i samband med folkomröstningen om Storbritanniens utträde ur EU år 2016).

Syftet med den här vägledningen är att ge en beskrivning av vad ni som politiska aktörer behöver tänka på utifrån kraven i EU:s dataskyddsförordning när ni behandlar personuppgifter i samband med valkampanjer och då särskilt vid användning av inriktnings- och förstärkningstekniker. Råden avser både hur ni som är ansvariga (personuppgiftsansvarig) och ni som anlitats i kampanjarbetet av dem som är ansvariga (personuppgiftsbiträde) följer reglerna om behandling av personuppgifter.

Informationen baseras i huvudsak på ställningstaganden från EU-domstolen, Europeiska dataskyddsstyrelsen (EDPB), särskilt Uttalande 2/2019 och Riktlinjer 08/2020 Targeting of social media users (användning av inriktnings- och förstärkningstekniker gentemot användare av sociala medier) och där sådana saknas ställningstaganden från IMY.

Information till de politiska partierna om valen finns på Valmyndighetens webbplats.

2 Checklista

Denna checklista kan användas av politiska aktörer som är ansvariga för hur personuppgifter behandlas i samband med valkampanjer. Som huvudregel gäller dataskyddsförordningen, men det finns vissa undantag.

Om dataskyddsförordningen är tillämplig behöver ni tänka på följande. Tänk även på att det krävs ett systematiskt arbete för att följa dataskyddreglerna och att reglerna gäller såväl *före, under som efter* en valkampanj.

1. **Kartlägg era personuppgiftsbehandlingar**. Detta är första steget för att kunna uppfylla kraven i dataskyddsförordningen.
2. **Fastställ särskilt och uttryckligen era ändamål med behandlingarna. Dokumentera ändamålen**. De sätter ramen för vad ni får göra med uppgifterna, exempelvis vilka uppgifter som är nödvändiga att behandla och hur länge. Det är utifrån de fastställda ändamålen ni kan bedöma om något undantag från era skyldigheter enligt dataskyddsförordningen är tillämpligt.
3. **Bedöm utifrån ändamålen om och i vilken mån era behandlingar är undantagna från kraven i dataskyddsförordningen**. Bedöm till exempel om er behandling undantas från kraven i dataskyddsförordningen på grund av att tillämpningen av förordningen skulle komma i konflikt med yttrandefrihetsgrundlagarna eller omfattas av undantaget för journalistiska ändamål.
4. **Följ de grundläggande dataskyddsprinciperna**. Till exempel följer av principen om uppgiftsminimering att det inte är tillåtet att behandla fler personuppgifter än vad som är nödvändigt för att uppnå ändamålen. Ändamålen ska vara berättigade och ni behöver kunna visa att ni följer principerna.
5. **Ni är ansvariga för den behandling som andra aktörer utför åt er**. Ni är ansvariga även för de behandlingar som era personuppgiftsbiträden utför på era instruktioner. Det gäller till exempel om ni anlitar en leverantör av tjänster för att genomföra valkampanjer och analyser på internet. Anlita inte aktörer som inte har kunskap om eller inte respekterar dataskyddsreglerna.
6. **För register över behandlingar** – både era egna och dem som andra utför åt er – om inte något undantag från denna skyldighet är tillämpligt. Registret ska vara skriftligt, tillgängligt i elektroniskt format, hållas uppdaterat och på begäran göras tillgängligt för IMY.
7. **Se till att ni har lagligt stöd för varje behandling** i någon av de rättsliga grunderna.
8. **Ta ställning till om ni kommer att behandla känsliga personuppgifter och se i så fall till att ni har stöd i ett undantag från förbudet att behandla sådana uppgifter**. Det gäller även uppgifter som avslöjar känsliga personuppgifter, alltså sådana uppgifter som skapas genom att dra slutsatser från och kombinera andra uppgifter. Ni behöver också kunna visa att ett undantag är tillämpligt.
9. Lämna **klar och tydlig information** till dem vars personuppgifter ni behandlar. Vid användning av inriktnings- och förstärkningstekniker bör relevant information lämnas till väljarna om varför de får ett visst budskap, vem som är personuppgiftsansvarig och hur de utövar sina rättigheter. Informationen ska ges i en klar, tydlig, begriplig och lätt tillgänglig form.
10. Se till att ni har bra **rutiner för att hantera enskildas begäranden** om att få utöva sina rättigheter. Det gäller särskilt rätten till tillgång, rättelse, radering och invändning. Tidpunkten för när en begäran kom in avgör vilka uppgifter ni behöver ge tillgång till. Om någon har begärt tillgång får ni inte radera uppgifter för att

slippa lämna ut dem om ni i samband med hanteringen av begäran upptäcker att behandlingen är olaglig. Enskilda har som huvudregel rätt att direkt till organisationer invända mot utskick som organisationerna gör för att främja sina mål och ideal. Detta torde även gälla politiska partier i sina valkampanjer, till exempel vid uppmaningar till väljare om att donera till eller stödja en valkampanj eller göra något, såsom att rösta på ett visst parti eller en viss kandidat.

11. **Ta ställning till om ni behöver göra en konsekvensbedömning**. Den ska göras innan ni inleder en behandling som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter. Det kan bli aktuellt om ni använder inriktnings- och förstärkningstekniker.
12. **Överför inte personuppgifter till tredjeland** om ni inte har stöd i ett giltigt överföringsverktyg i dataskyddsförordningen.

3 När gäller dataskyddsförordningen (GDPR)?

Dataskyddsförordningen är som huvudregel tillämplig på all behandling av personuppgifter. Det innebär att dataskyddsförordningen har ett mycket brett tillämpningsområde då alla uppgifter som gör att en levande person direkt eller indirekt kan identifieras är personuppgifter och i princip allt som kan göras med personuppgifter, även ren lagring, är en behandling. Syftet med regleringen i dataskyddsförordningen är att skydda enskilda personers integritet.

Ni som behandlar personuppgifter är antingen personuppgiftsansvarig eller personuppgiftsbiträde. Personuppgiftsansvarig är den som bestämmer för vilka ändamål (syften) uppgifterna ska behandlas och hur behandlingen ska gå till. Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvarigas räkning. Om två eller flera gemensamt bestämmer över en viss behandling kan de vara gemensamt personuppgiftsansvariga och behöver sinsemellan bestämma vem som är ansvarig för att fullgöra de olika skyldigheterna i dataskyddsförordningen.

Tänk på att ni behöver följa regleringen i dataskyddsförordningen även i samband med valkampanjer. Förordningen innehåller dock vissa undantag. Vid behandling av personuppgifter i samband med valkampanjer är det framför allt undantaget för journalistiska ändamål som kan bli tillämpligt (se vidare under rubriken ”Undantag för journalistiska ändamål när TF och YGL inte är tillämpliga”).

3.1 Undantag med hänsyn till yttrande- och informationsfriheten

3.1.1 Förhållandet till tryckfrihetsförordningen och yttrandefrihetsgrundlagen

Enligt dataskyddsförordningen är medlemsstaterna skyldiga att genom nationell lagstiftning förena rätten till skydd för den personliga integriteten och rätten till yttrande- och informationsfrihet. I den svenska lagen som kompletterar dataskyddsförordningen anges att personuppgiftsbehandling som omfattas av grundlagsskyddet i tryckfrihetsförordningen (TF) och yttrandefrihetsgrundlagen (YGL) undantas från kraven i dataskyddsförordningen om tillämpningen av förordningen skulle komma i konflikt med grundlagarna.

TF och YGL förbjuder det allmänna (till exempel myndigheter) att hindra spridning av grundlagsskyddade publiceringar, det så kallade hinderförbudet. Det innebär

exempelvis att spridning av tryckt politisk reklam till allmänheten eller en större grupp enskilda är skyddad mot ingripanden från det allmänna.

Exempel 1: Det politiska partiet YY vill skicka tryckt politisk marknadsföring till alla som bor i Jönköpings län. För att nå ut till mottagarna behandlas deras personuppgifter genom ett utdrag från det statliga personadressregistret (SPAR) där mottagarens adressuppgifter och namn framgår. Namn och adress trycks på kuvert som skickas med post. IMY får inte med stöd av dataskyddsförordningen ingripa mot den behandling av personuppgifter som sker vid partiets utskick av trycksaken, eftersom det skulle strida mot hinderförbudet. Däremot omfattas den personuppgiftsbehandling som sker vid partiets utdrag från SPAR av reglerna i dataskyddsförordningen.

3.1.2 Undantag för journalistiska ändamål när TF och YGL inte är tillämpliga

I den svenska lagen som kompletterar dataskyddsförordningen görs undantag från vissa angivna bestämmelser i dataskyddsförordningen med hänsyn till yttrande- och informationsfriheten även för sådana yttranden som inte omfattas av TF och YGL. Undantaget omfattar behandlingar som sker för journalistiska ändamål. Är undantaget tillämpligt gäller således inte de merparten av bestämmelserna i dataskyddsförordningen. Undantaget omfattar dock inte de bestämmelser i dataskyddsförordningen som gäller för säkerhet i samband med behandlingen.

Uttrycket ”journalistiska ändamål” ska ges en vid tolkning och omfattar yttranden med syfte att sprida information, åsikter eller idéer till allmänheten. Undantaget gäller också för andra än yrkesverksamma journalister och omfattar, enligt IMY:s bedömning, exempelvis den åsiktsbildning och det opinionsbildande som politiska partier ägnar sig åt. Uttrycket ”journalistiska ändamål” har alltså i detta sammanhang en bredare betydelse än vad det har i vardagligt språkbruk.

Undantaget omfattar även rätten att framföra yttranden, åsikter, information och tankar som kan uppfattas som chockerande eller störande.

Undantaget omfattar inte spridning av rent privata uppgifter. Var gränsen går för vad som är rent privata uppgifter varierar beroende på sammanhanget och vilken roll den berörda personen har (t.ex. privatperson eller riksdagsledamot).

Spridning av ett politiskt budskap som innehåller personuppgifter kan omfattas av undantaget för journalistiska ändamål.

Exempel 2: AA publicerar en serie inlägg på sina konton i sociala medier om varför de röstberättigade i kommunen borde välja AA till kommunalråd i valet och inte det sittande kommunalrådet BB. I inläggen informerar AA om och kritiserar hur BB agerat i sin politiska gärning och lyfter fram hur AA själv skulle ha agerat och hur AA kommer att agera om AA blir vald. Några av inläggen innehåller även mer privata uppgifter om BB, till exempel att upprepade uteblivna betalningar för fordringsanspråk för renoveringar av BB:s sommarstuga har gått till Kronofogden. AA försvarar publiceringen av uppgifterna med att de vittnar om BB:s bristande omdöme som är olämpligt för en hög politisk befattningshavare. Dessutom vill AA

väcka allmän debatt kring vad AA anser vara en utbredd nonchalans från politiker i ledande befattningar för krav som andra ”vanliga” medborgare förväntas följa.

Enligt IMY:s mening omfattas denna behandling av journalistiska ändamål, även de mer privata uppgifterna om skulder till Kronofogden. Anledningen till att även de privata uppgifterna omfattas är att BB som politiker medvetet och frivilligt har valt att delta i det offentliga livet. BB behöver därför acceptera att det kan finnas ett samhällsintresse av att allmänheten kan ta del av vissa uppgifter om BB som skulle anses vara rent privata för personer som inte har en roll i det offentliga livet.

Behandling av *mottagarnas* personuppgifter inför spridningen av politiska budskap, till exempel vid den profilering som sker i samband med att inriktnings- och förstärkningstekniker används vid urval av mottagare, omfattas enligt IMY:s bedömning inte av undantaget för journalistiska ändamål.

Exempel 3: Valet närmar sig och det politiska partiet YY vill till väljarna i en region skicka ut information om valet och partiets politik. För att nå ut till så många som möjligt och begränsa kostnaderna vill YY skicka informationen med sms. YY samlar därför in namn och postadress från den officiella vallängden och Statens personadressregister (SPAR) och kompletterar med mobiltelefonnummer via en samarbetspartner utifrån öppna tillgängliga källor och skickar sedan informationen med sms.

Enligt IMY:s bedömning omfattas inte behandlingen av undantaget för journalistiska ändamål. YY behöver därför följa reglerna i dataskyddsförordningen, bland annat ha en rättslig grund för insamlingen och följa de grundläggande principerna.

Om ni stödjer er personuppgiftsbehandling på undantaget för journalistiska ändamål bör ni vara tydliga med det i er information till enskilda. Det gäller till exempel i besked till enskilda som nekas att utöva sina rättigheter med stöd av undantaget. Ni bör också informera enskilda om möjligheten att lämna in ett klagomål till IMY. Det är viktigt för att väljarna ska förstå varför deras begäranden enligt dataskyddsförordningen, till exempel invändningar och frågor, inte hanteras. Det är också viktigt för att IMY ska kunna bedöma om det finns anledning att inleda tillsyn med anledning av sådana klagomål.

4 När dataskyddsförordningen gäller

Om något undantag inte är tillämpligt gäller dataskyddsförordningen fullt ut för den behandling av personuppgifter som sker i samband med olika typer av valkampanjer.

Om ni, eller någon som agerar på ert uppdrag, till exempel betalar en leverantör av ett socialt medium för att välja ut användare av mediet utifrån särskilda egenskaper (det vill säga använder er av inriktnings- och förstärkningstekniker), behöver ni alltså följa dataskyddsförordningen.

Exempel 4: CC kontaktar det politiska partiet YY för att få veta vad ett eventuellt medlemskap i partiet skulle innebära. CC kontaktar partiet via mejl för att boka ett möte med en av partiets representanter. Efter mötet beslutar CC att inte bli medlem i partiet. Partiet har dock lagt till CC:s mejladress i sin lista med mejladresser till potentiella medlemmar. Partiet samkör sedan listan med mejladresser med dem som ett socialt medium har, för att nå ut till berörda personer med information om varför de bör rösta på partiet genom riktad marknadsföring på det sociala mediet. Partiets behandling av CC:s personuppgifter behöver ske i enlighet med dataskyddsförordningen.

Ni behöver följa reglerna i dataskyddsförordningen även vid annan behandling som sker i samband med politisk marknadsföring, exempelvis när analyser görs av de mottagare som tagit del av eller visat uppskattning för viss politisk marknadsföring (till exempel ”gilla-markeringar” i sociala medier) för att göra prognoser om den förväntade valutgången.

Om ni behandlar personuppgifter i samband med valkampanjer bör ni tänka på att:

- följa de grundläggande principerna (avsnitt 4.1)
- ha en rättslig grund för behandlingen (avsnitt 4.2)
- ni är ansvariga om behandlingen utförs av någon annan men för er räkning (avsnitt 4.3)
- det finns risk att känsliga personuppgifter behandlas (det vill säga bland annat uppgifter om politiska åsikter och medlemskap i fackförening) och oavsett om det är avsiktligt eller inte krävs stöd i ett undantag från förbudet att behandla sådana uppgifter (avsnitt 4.4)
- väljarna ska informeras om behandlingen och ges rätt att utöva sina rättigheter (avsnitt 4.5)
- en konsekvensbedömning förmodligen behöver göras innan behandlingen påbörjas om ni använder inriktnings- och förstärkningstekniker (avsnitt 4.6)
- om ni överför personuppgifter till tredjeland behöver ni kunna visa att något av de verktyg som anges i kapitel V i dataskyddsförordningen kan användas för att överföra uppgifterna så att ni inte undergräver den skyddsnivå för de registrerades personuppgifter som garanteras i EU/ESS-området (avsnitt 4.7).

4.1 De grundläggande principerna

De grundläggande principerna är kärnan i dataskyddsförordningen. Principerna gäller för all personuppgiftsbehandling och sätter de yttersta ramarna för vad som är en tillåten behandling. Dessa är principerna om:

- laglighet
- korrekthet
- öppenhet
- ändamålsbegränsning
- uppgiftsminimering
- riktighet
- lagringsminimering
- integritet och konfidentialitet (säkerhet).

Dessutom finns ansvarsprincipen. Den innebär att om ni är personuppgiftsansvarig för behandlingen, behöver ni kunna visa att principerna följs. Det gäller även för behandlingar som utförs på ert uppdrag av andra (personuppgiftsbiträden). Det är därför viktigt att ni dokumenterar era behandlingar, överväganden och åtgärder.

Principen om laglighet innebär att det ska finnas en rättslig grund för behandlingen (se nästa avsnitt). Även övriga bestämmelser i dataskyddsförordningen behöver följas.

Principen om korrekthet innebär att behandlingen av personuppgifter ska vara rättvis, skälig och rimlig i förhållande till de registrerade. Den ska också stå i rimlig proportion till nyttan som den innebär och inte strida mot de registrerades rimliga förväntningar. Behandlingen ska vara förståelig och begriplig för de registrerade och inte ske på dolda eller manipulerande sätt.

Exempel 5 – korrekthet: Det politiska partiet YY sammanställer en lista över användare på sociala medier som har "gillat" vissa typer av inlägg som tyder på att de har en viss politisk åsikt och laddar upp listan till ett socialt medium för att mediet ska kunna rikta politisk reklam från YY till liknande personer (så kallade lookalike-målgrupper). Det strider enligt IMY:s bedömning mot principen om korrekthet. En sådan behandling kan nämligen gå utöver användarnas rimliga förväntningar.

Principen om öppenhet innebär att det ska vara klart och tydligt för de registrerade att, hur och varför deras personuppgifter behandlas. De ska också få information om vad de har för rättigheter, till exempel hur uppgifter kan rättas eller raderas. Informationen ska vara lätt att hitta och formulerad på ett enkelt och begripligt sätt.

Exempel 6 – korrekthet, öppenhet och ändamålsbegränsning: DD gör ett yrkeslämplighetsprov som tagits fram av företaget XX AB. Provet innehåller en psykologisk utvärdering som finns på ett socialt medium och använder det programmeringsgränssnitt (API) som erbjuds av leverantören av det sociala mediet. XX AB samlar in uppgifter om DD:s utbildning, anställningsstatus, ålder, hobbyer, inlägg, mejladress och kontakter. XX AB får uppgifterna via API:n i enlighet med det godkännande som DD lämnat via sitt konto på det sociala mediet. Det uttalade syftet med applikationen är att förutsäga vilken karriärväg som är bäst för en viss användare. Utan det sociala mediets vetskap eller godkännande använder XX AB informationen för att dra slutsatser om ett antal personliga aspekter, däribland DD:s personlighetsdrag och politiska övertygelser. XX AB vill att det politiska partiet YY ska vinna valet och beslutar därför senare att baserat på informationen skicka marknadsföring för partiet till DD. XX AB använder den e-postbaserade funktionen för sådana tekniker som det sociala mediet erbjuder för att rikta marknadsföringen, utan att lägga till några andra kriterier som erbjuds av det sociala mediet.

Genom att agera på detta sätt behandlar XX AB känsliga personuppgifter (se mer om vad som kan vara känsliga personuppgifter nedan), men det gör inte det sociala mediet. Bedömningen och identifieringen av DD:s politiska övertygelse sker utan medverkan från det sociala mediet. Förutom att behandla känsliga personuppgifter strider användningen av inriktnings- och förstärkningstekniker mot kraven på korrekthet, öppenhet och ändamålsbegränsning. DD har inte blivit

informerad om att DD:s personuppgifter kommer att behandlas för att rikta politisk reklam till DD. Förfarandet verkar enligt IMY:s bedömning dessutom inte vara förenligt med ändamålet att erbjuda ett yrkeslämplighetsprov och alltså i strid med strider därmed mot principen om ändamålsbegränsning.

Principen om ändamålsbegränsning innebär att personuppgifter bara får samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Principen innebär att ändamålen behöver

- ha bestämts innan behandlingen påbörjas
- vara specifika och konkreta och inte för allmänt hållna
- komma till utryck på ett tydligt sätt till exempel genom att dokumenteras
- garantera en laglig behandling av personuppgifter, det vill säga att det ska finnas en rättslig grund.

Tydligt angivna ändamål är en förutsättning för att det ska kunna bedömas om en viss behandling är laglig, det vill säga om den är nödvändig i något av de sammanhang som räknas upp som rättsliga grunder utöver samtycke. Av principen följer också att om ni samlar in uppgifter för ett visst ändamål, får ni endast behandla uppgifterna för andra ändamål om de är förenliga med ändamålen för den första behandlingen. Ni behöver därför göra en så kallad förenlighetsbedömning, där ni ska väga in:

- kopplingar mellan det ursprungliga och det nya ändamålet
- de enskildas rimliga förväntningar utifrån det sammanhang inom vilket personuppgifterna har samlats in
- uppgifternas art, särskilt om känsliga personuppgifter eller brottsuppgifter behandlas
- eventuella konsekvenser för väljarna av den planerade fortsatta behandlingen
- förekomsten av lämpliga tekniska och organisatoriska skyddsåtgärder (som vid behandling för andra ändamål i vissa fall kan kompensera för konsekvenserna för väljarna och ändå säkerställa en korrekt behandling).

Exempel 7 – ändamålsbegränsning: Det politiska ungdomsförbundet ZZ är ute och värvar medlemmar på en gymnasieskola. Vid besöket erbjuder ZZ eleverna möjlighet att anmäla sig för att få uppdateringar om ungdomsförbundets framtida evenemang via mejl. ZZ vill sedan ladda upp mejladresserna till ett socialt medium för att kunna använda det sociala mediets inriktnings- och förstärkningstekniker för att rikta politisk marknadsföring till liknande personer (så kallade lookalike-målgrupper). Här är användningen av uppgifterna i det sociala mediet en fråga om ett annat ändamål än det som uppgifterna ursprungligen samlades in för. ZZ behöver därför inhämta ett samtycke för det nya ändamålet, då det inte är förenligt med det ursprungliga av följande skäl:

- Det ursprungliga ändamålet (erbjuda uppdateringar om evenemang) och det nya (rikta marknadsföring till liknande personer) sammanfaller inte och saknar en logisk koppling.
- Det nya ändamålet framstår som överraskande och osannolikt för de potentiella medlemmarna utifrån *rimliga förväntningar från det sammanhang* som uppgifterna ursprungligen samlades in.

- *Uppgifternas art* kan utöver mejladress antas inbegripa slutsatser om känsliga uppgifter (politiska åsikter).
- Utlämnandet av uppgifterna till det sociala mediet innebär negativa *konsekvenser* för de potentiella medlemmarna (det finns risk för att uppgifterna samkörs med andra uppgifter som det sociala mediet redan har om dem och att de profileras för att få riktad reklam).
- ZZ har inte vidtagit några skyddsåtgärder, såsom till exempel kryptering eller pseudonymisering.

Principen om uppgiftsminimering innebär att personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet. Behandla aldrig fler personuppgifter än vad som behövs. De personuppgifter som behandlas ska vara tydligt kopplade till ändamålet.

Principen om riktighet innebär att de personuppgifter som behandlas ska vara riktiga och, om nödvändigt, uppdaterade. Om personuppgifterna inte stämmer ska ni rätta eller radera dem.

Principen om lagringsminimering innebär att ni bara får spara personuppgifter så länge som de behövs för ändamålet med personuppgiftsbehandlingen. När personuppgifterna inte längre behövs för ändamålet ska ni radera eller avidentifiera dem. Ni bör därför införa rutiner för gallring av personuppgifter, till exempel att ni genomför regelbundna kontroller eller raderar efter viss tid.

Principen om integritet och konfidentialitet (säkerhet) innebär att alla personuppgifter som ni behandlar behöver skyddas, så att ingen obehörig kommer åt dem och så att de inte används på ett otillåtet sätt. Ni ska också se till så att personuppgifter inte förloras eller blir förstörda, till exempel genom olyckshändelser.

4.2 Rättslig grund

Den som behandlar personuppgifter behöver stödja sig på någon av de rättsliga grunderna för att behandlingen ska vara laglig. Dataskyddsförordningen innehåller sex rättsliga grunder, bland annat samtycke, intresseavvägning och avtal. De rättsliga grunder som främst kan tänkas bli aktuella i samband med valkampanjer är samtycke och intresseavvägning.

4.2.1 Samtycke

För att ett samtycke ska vara giltigt krävs för det första att följande är uppfyllt: samtycket är *frivilligt*, *specifikt*, *informerat* och ger uttryck för en *otvetydig viljeyttring*.

Med *frivilligt* menas att ha kontroll och möjlighet att välja fritt. Tumregeln är att enskilda ska ha möjlighet att välja fritt och till exempel inte ska känna sig tvingade eller få utstå negativa konsekvenser om de inte samtycker. Samtycket får inte heller vara en obligatorisk del av avtalsvillkor. Enskilda behöver också kunna vägra att samtycka eller ta tillbaka sitt samtycke utan att drabbas av problem eller negativa konsekvenser. Samtycket är till exempel inte frivilligt om valet består av att välja mellan att samtycka till personuppgiftsbehandling för att använda en tjänst eller att välja en likvärdig tjänst som erbjuds av någon annan, då valfriheten i så fall skulle bero på vad andra aktörer på marknaden gör och om en viss person anser att den andra tjänsten är helt likvärdig. Det ska också beaktas om förhållandet mellan den enskilda och den

personuppgiftsansvariga är ojämlikt, till exempel på grund av ett anställningsförhållande, eftersom det kan innebära att valet inte är fritt.

Med *specifikt* menas att samtycket lämnas för ett eller flera specifika ändamål och att den enskilda har en valmöjlighet ifråga om vart och ett av dessa ändamål.

Med *informerat* menas att enskilda ska ha fått information i förväg för att kunna fatta informerade beslut och förstå vad de går med på. Informationen ska vara lättillgänglig och anpassad till målgruppen. Den ska vara lättbegriplig för gemene man.

Ni behöver tänka på att inte använda långa integritetspolicyer eller meddelanden som är svåra att förstå. Begäran om samtycke behöver läggas fram på ett sätt som klart och tydligt kan särskiljas från andra frågor och får till exempel inte ingå som en punkt i avtalsvillkor.

Informationen behöver i varje fall innehålla:

- vem som är personuppgiftsansvarig
- syftet med behandlingen
- vilken typ av information som kommer att samlas in och användas
- möjligheten att återkalla samtycket
- om uppgifterna används för automatiserat beslutsfattande
- eventuella risker om uppgifterna överförs till tredjeland.

Med *otvetydig viljeyttring* avses att samtycket alltid behöver ges aktivt eller genom en förklaring. Det innebär att den som samtycker behöver ha utfört en medveten handling (det vill säga en entydig och bekräftande handling), till exempel kryssat i en kryssruta på en webbplats. Förifyllda kryssrutor är inte tillåtna, eftersom det inte ger uttryck för ett aktivt beteende och lika gärna kan vara något som den enskilda missat att reagera på. Exempelvis är det inte tillräckligt att den enskilda scrollar eller svajpar igenom en webbsida, då sådana handlingar kan vara svåra att skilja från andra handlingar eller interaktion vilket inte gör det möjligt att avgöra om ett entydigt samtycke har lämnats. Tystnad, inaktivitet eller enbart utnyttjande av en tjänst är inte aktiva val. Samtycke kan inte heller anses ha lämnats av den enskilde genom att godta ett avtal eller allmänna villkor för en viss tjänst.

Samtycke kan lämnas genom en skriftlig eller (inspelad) muntlig förklaring, inklusive på elektronisk väg. Sådana samtyckesförklaringar kan vara utformade på flera olika sätt och vara olika omfattande för att uppfylla kraven.

Exempel 8: När det politiska ungdomsförbundet ZZ var ute och värvade medlemmar till förbundet på gymnasieskolan samlade ZZ in uppgifterna med stöd av samtycke. För att se till att samtycket var frivilligt, specifikt, informerat och ett uttryck för en otvetydig viljeyttring gjorde ZZ följande:

- ZZ var tydliga med att det var frivilligt att anmäla sig och inhämtade samtycke för att använda mejladresserna endast för ändamålet att skicka uppdateringar om ZZ:s framtida evenemang.
- Samtycket inhämtades genom blanketter som frivilligt fylldes i av intresserade elever där de fick kryssa i en kryssruta.

I blanketten informerades de skriftligt om att ZZ är personuppgiftsansvarig, att det endast är namn och mejladress som samlas in, att syftet med behandlingen är att uppdatera dem om ZZ:s framtida evenemang, hur de enkelt kan återkalla samtycket och att uppgifterna inte överförs till tredjeland.

För det andra behöver ni *kunna visa att samtycke faktiskt har lämnats*. Hur ni gör det är inte exakt reglerat utan kan anpassas till förutsättningarna i er verksamhet. Dokumentationen ska inte i sig leda till att er behandling av personuppgifter ökar på ett onödigt sätt. Er dokumentation bör innehålla tillräckliga uppgifter för att visa en koppling mellan samtycket och behandlingen, men inte fler uppgifter än nödvändigt. Ni behöver kunna visa att samtycke har lämnats så länge som behandlingen pågår. Därefter bör samtyckesbeviset inte bevaras längre än vad som är strikt nödvändigt för att uppfylla en rättslig förpliktelse (till exempel kunna visa att ni efterlever dataskyddsförordningen) eller för att kunna fastställa, göra gällande eller försvara rättsliga anspråk. Ni kan till exempel föra ett register över samtyckesförklaringar, så att ni kan visa hur och när ni fick samtycket och den information som då lämnades. Ni ska också kunna visa att enskilda har informerats och att era arbetsflöden har uppfyllt alla relevanta kriterier för ett giltigt samtycke.

Och för det tredje krävs *att samtycket kan återkallas* och då lika lätt som det var att lämna samtycket. Om samtycke lämnats elektroniskt genom ett musklick, ett knapptryck, en svajp eller ett tangenttryck behöver de enskilda i praktiken kunna återkalla samtycket lika lätt. Om ni inhämtar samtycke genom enkla åtgärder för enskilda kan det vara svårt för er att erbjuda ett sätt för att återkalla samtycket som är lika enkelt. Om ni inhämtat samtycket genom ett tjänstspecifikt användargränssnitt (till exempel via en webbplats eller app) behöver samtycket kunna återkallas via samma elektroniska gränssnitt. Det behöver kunna återkallas utan problem, till exempel inte kosta något eller innebära att en tjänst försämras.

Exempel 9: Partiet YY säljer biljetter till sitt politiska friluftsläger i sin webbshop. För varje biljett som säljs krävs samtycke för att få använda kontaktuppgifterna i reklamsyfte. Kunderna kan svara ”Ja” eller ”Nej” på frågan om de samtycker eller ej. YY informerar kunderna om att de har möjlighet att återkalla sitt samtycke. För att göra detta kan de kontakta en teletjänstcentral på arbetsdagar kl. 08.00–17.00 utan kostnad. Genom att göra så har dock YY inte erbjudit kunden ett sätt att återkalla sitt samtycke lika lätt som det varit att lämna det.

För att återkalla samtycket måste telefonsamtalet göras under arbetstid, vilket är mer mödosamt än det musklick som krävs för att lämna samtycket på nätet direkt i webbshoppen, som har öppet 24 timmar om dygnet, 7 dagar i veckan.

Det finns även något som kallas *uttryckligt samtycke* och som krävs när den registrerade ska lämna samtycke till behandling av känsliga personuppgifter (se nedan under rubriken undantag för att behandla känsliga personuppgifter).

4.2.2 Intresseavvägning

Om ni vill stödja er behandling på den rättsliga grunden intresseavvägning (även kallad berättigade intressen) krävs att ni kan visa att tre villkor är uppfyllda:

- det finns ett eller flera *berättigade intressen*
- behandlingen av personuppgifter är *nödvändig* för ett ändamål som rör de berättigade intressena
- de registrerades intressen eller grundläggande fri- och rättigheter *väger inte tyngre* än de berättigade intressena (intresseavvägning).

Vad som kan vara ett *berättigat* intresse ska tolkas brett. Avgörande är om intresset är tillåtet i lagstiftning eller annars allmänt erkänt i ett rättssamhälle. Obetydliga intressen väger inte lika tungt som viktiga eller tvingande intressen, men är något som får betydelse först vid själva intresseavvägningen. Om ett intresse *inte* är berättigat ska dock intresseavvägningen inte utföras, eftersom den ursprungliga tröskeln för denna rättsliga grund inte kommer att ha uppnåtts.

Exempel 10 – oberättigat intresse: Partiet ÅÅ:s enda intresse av en viss behandling av personuppgifter genom inriktnings- och förstärkningstekniker i sociala medier är att diskriminera väljare av en viss etnicitet, för ändamålet att förmå väljare av denna etnicitet, som typiskt sett inte röstar på partiet, att inte rösta i valet. Ett sådant intresse kan aldrig vara berättigat och göra personuppgiftsbehandlingen tillåten.

Det ska också vara fråga om ett *faktiskt intresse* vid tidpunkten för behandlingen och inte ett intresse som är hypotetiskt vid den tidpunkten. Om det finns omständigheter som visar att intresset inte är hypotetiskt är villkoret uppfyllt, men det kan även vara tillräckligt att intresset typiskt sett framstår som faktiskt.

Exempel 11 – faktiskt intresse: Partiet YY håller ett torgmöte där partiets kandidater talar och tar i samband med mötet foton på talarna. På torget i bakgrunden kan förbigående personer ses som eventuellt kan identifieras. YY:s ändamål med behandling av de förbipasserande personernas personuppgifter är att få material till informationsbroschyrer och sociala medier för att informera om partiets verksamhet, vilket rör det berättigade intresset att sprida information om partiets verksamhet. Intresset är faktiskt och inte hypotetiskt.

Exempel 12 – hypotetiskt intresse: Efter torgmötet går volontärer från partiet YY:s ungdomsförbund ZZ igenom partiets publiceringar på sociala medier från torgmötet och upprättar en lista över alla användare i sociala medier som har ”gillat” publiceringarna och skickar listan till partiet. ZZ menar att de gör detta med stöd av *partiets* intresse av att kunna skicka information om partiets kandidater till användarna. Det är dock inget berättigat intresse utan hypotetiskt vid tidpunkten för behandlingen, då det finns en risk att partiet inte vill ha informationen eller är intresserade av att skicka någon sådan information.

Att behandlingen ska vara *nödvändig* innebär att de intressen som behandlingen avser att skydda inte rimligen skulle kunna skyddas på ett lika effektivt sätt genom andra medel som i mindre utsträckning inkräktar på de registrerades grundläggande fri- och rättigheter. Villkoret ska prövas tillsammans med principen om uppgiftsminimering (se

ovan) och innebär bland annat att personuppgifter inte ska behandlas i onödan eller att uppgifterna sparas för att de ”kan vara bra att ha”.

Exempel 13 – onödig behandling: I exempel 11 med torgmötena ovan går volontärer från partiet runt och fotograferar och tar namn på samtliga åhörare och förbipasserande. Dessa behandlingar är inte nödvändiga för att skydda partiets intresse av att kunna informera om sin verksamhet.

Det tredje villkoret, *intresseavvägning*, görs genom en helhetsbedömning, där det särskilt ska vägas in:

- allvaret i den kränkning som behandlingen innebär för de registrerade
- vad registrerade rimligen kan förvänta sig i situationen och
- vilka skyddsåtgärder som vidtagits.

Exempel 14 – samtliga steg: I exempel 3 ovan konstateras att partiet YY behöver följa dataskyddsförordningen när partiet samlar in telefonnummer och skickar sms till väljarna i regionen. YY vill stödja behandlingarna på den rättsliga grunden intresseavvägning.

Enligt YY är det *berättigade intresset* partiets intresse av att sprida information om sin politik och verksamhet till de röstberättigade i regionen. Enligt IMY:s mening är ett sådant intresse berättigat och YY kan därför gå vidare till nästa steg.

YY behöver i det andra steget, *nödvändighet*, fundera på om behandlingen är nödvändig genom att fråga sig om intresset inte rimligen kan tillgodoses på ett lika effektivt sätt genom att utföra färre personuppgiftsbehandlingar eller behandla färre uppgifter, till exempel bara uppgifter om postadress. Argument som talar för att det är nödvändigt kan till exempel vara kopplade till att somliga inte har möjlighet att eller kommer att ta del av utskick som görs med post. I detta behöver YY även beakta principen om uppgiftsminimering och minimera de behandlade uppgifterna i möjligaste mån– till exempel till bara de röstberättigade i regionen – som krävs för att YY ska kunna uppnå ändamålet. YY behöver också se till att uppgifterna inte behandlas längre än vad som är nödvändigt, till exempel radera uppgifterna direkt efter att utskicket genomförts. Om YY kommer fram till att behandlingen faktiskt är nödvändig kan YY gå vidare till nästa steg.

I det tredje steget, *intresseavvägningen,* behöver YY för det första särskilt fundera kring vad som kan ligga i väljarnas *rimliga förväntningar*, alltså om enskilda typiskt sett kan förvänta sig en behandling som den aktuella. Här kan det vara av betydelse om YY har några konkreta uppgifter som talar för detta. Till exempel kanske YY kan hänvisa till eller har låtit utföra en extern opinionsundersökning i ett representativt urval av väljare, som visar att de flesta förstår att sådan behandling kan komma att ske i anslutning till allmänna val och inte upplever den som integritetskränkande om de samtidigt får information om den och om vem som är avsändaren. Dessutom kanske en sådan visar att flera deltagare till och med föredrar att få informationen på detta sätt istället för i brevlådan.

För det andra behöver YY bedöma *allvaret i kränkningen* som behandlingen innebär. Om det till exempel är fråga om mobiltelefonnummer till personer som inte

har hemligt nummer och som finns tillgängliga i öppna källor, minskar det allvaret i den rättighetskränkning som det innebär för väljarna att få sina personuppgifter behandlade. YY bör också bedöma om uppgifterna i sig är integritetskänsliga och till exempel kombineras med andra uppgifter än de registrerades namn, postadress och att de är röstberättigade i valet. Här behöver YY vara särskilt uppmärksamma på om urvalet kopplas till känsliga uppgifter, till exempel om faktiska eller antagna politiska åsikter.

YY behöver för det tredje bedöma riskerna för väljarnas grundläggande fri- och rättigheter och om de kan minskas genom att YY vidtar *skyddsåtgärder*. Till exempel kan YY fundera på om de kan minska det obehag som några skulle kunna tänkas känna av att få sådana utskick genom att se till att det tydligt framgår att det är YY som är avsändare och att det finns mer information om behandling i YY:s integritetspolicy som finns på partiets webbplats. YY kan också överväga att se till att ha och informera om sina välfungerande funktioner för dem som vill spärra sig för utskick från partiet – både vid för- och efterhand – och om möjligt lämna mer information än vad som krävs enligt dataskyddsförordningen. Om YY efter att ha gjort detta kommer fram till att väljarnas intresse eller grundläggande fri- och rättigheter inte väger tyngre än de berättigade intresset – och därmed inte kräver skydd av väljarnas personuppgifter – så är behandlingen tillåten.

Slutligen behöver YY dokumentera dessa överväganden så att partiet kan visa att de följer ansvarsprincipen.

4.3 Behandlingar som utförs på uppdrag av andra och gemensamt ansvar

Den som är personuppgiftsansvarig ansvarar ytterst för att andra som behandlar personuppgifter på deras uppdrag följer reglerna. De får inte anlita andra som inte kan säkerställa att reglerna följs.

Exempel 15: Det politiska partiet YY funderar på att anlita en reklambyrå för att utforma kampanjer och åtgärder som inbegriper att betala en leverantör av ett socialt medium för att skicka politisk reklam till väljare. Reklambyrån har dock inte koll på dataskyddsreglerna och vill därför inte ingå något personuppgiftsbiträdesavtal med YY. YY vet att partiet skulle vara personuppgiftsansvarig och ytterst ansvarigt för hur reklambyrån behandlar personuppgifter på YY:s vägnar och avstår därför från att anlita den.

Om ni använder er av inriktnings- och förstärkningstekniker för att rikta marknadsföring anses ni normalt vara gemensamt personuppgiftsansvarig med den som erbjuder sådana funktioner för delar av behandlingen. Ni behöver därför ingå ett så kallat ”gemensamt arrangemang”. Ett gemensamt arrangemang innebär att ni under öppna former ska bestämma ert respektive ansvar för att fullgöra era skyldigheter enligt dataskyddsförordningen, särskilt ifråga om utövandet av de registrerades rättigheter och era respektive skyldigheter att ge den information som krävs. Inom ramen för arrangemanget får ni utse en gemensam kontaktpunkt för de registrerade. Arrangemanget ska på ett lämpligt sätt återspegla era respektive roller och

förhållanden gentemot registrerade. Ni ska göra det väsentliga innehållet i arrangemanget tillgängligt för de registrerade. Oavsett formerna för arrangemanget får dock de registrerade utöva sina rättigheter gentemot var och en av er.

Det finns inget krav på att det gemensamma arrangemanget ska komma till uttryck i ett skriftligt avtal eller liknande mellan de ansvariga. För att öka säkerheten för både er och de enskilda rekommenderar dock IMY att det kommer till uttryck i ett bindande dokument, för att ni ska kunna uppfylla kraven i principerna om öppenhet och ansvar.

Exempel 16: Partiet YY vill rikta politisk marknadsföring i ett socialt medium till väljarna och bestämmer sig för att göra det utan någon mellanhand. YY ingår ett inbördes gemensamt arrangemang med det sociala mediet, som särskilt rör information till väljarna om kriterier för urvalet av marknadsföringen. Innehållet i arrangemanget görs tillgängligt för väljarna genom en hänvisning till integritetspolicyn och en länk på det sociala mediet med rubriken ”Varför ser jag denna annons?”.

YY ser även till att informera väljarna om att deras mejladresser kommer att användas för reklam via det sociala mediet med information kopplad till YY. All vidare behandling som utförs av det sociala mediet behöver vara laglig och förenlig med de ändamål för vilka YY samlade in uppgifterna.

I den mån det sociala mediet planerar att behandla väljarnas mejladresser ytterligare i ett annat syfte behöver det sociala mediet se till att väljarna får den information som krävs i dataskyddsförordningen innan detta görs. YY och det sociala mediet kan komma överens om att YY ska ge relevant information till väljarna på uppdrag av det sociala mediet. Det sociala mediet är dock ytterst ansvarigt för att se till att väljarna har fått information om all behandling som det sociala mediet (ensamt) ansvarar för.

Exempel 17: DD surfar in på YY:s webbplats och tittar på YY:s information om medlemskap och partipolitik, men beslutar att inte gå med i partiet. YY vill rikta marknadsföring till användare av ett socialt medium som har besökt partiets webbplats utan att gå med i partiet, det vill säga väljare såsom DD.

I detta syfte har YY lagt in en så kallad spårningspixel på sin webbplats som tillhandahålls av det sociala mediet. En spårningspixel består av programmeringskod som en webbplatsinnehavare (såsom YY) kan integrera på sin webbplats, som gör att när en person besöker webbplatsen kommer dennes webbläsare automatiskt hämta en fil från en server (i det här fallet det sociala mediet). När pixeln väl laddats ned så kan det sociala mediet typiskt sett övervaka användarens besök på webbplatsen, till exempel för att lägga till personen i en viss målgrupp för att rikta reklam till.

Efter att ha lämnat YY:s webbplats och loggat in på sitt konto på det sociala mediet börjar DD i enlighet därmed se reklam för YY på det sociala mediet.

IMY konstaterar här att det gemensamma arrangemanget mellan YY och det sociala mediet bör omfatta all behandling av personuppgifter där det föreligger gemensamt personuppgiftsansvar. Det inkluderar allt från insamlingen av

personuppgifter i samband med DD:s besök på YY:s webbplats med spårningspixeln till visningen av annonserna för DD på sociala medier. Det inkluderar även eventuell statistik från den riktade marknadsföringskampanjen.

4.4 Känsliga personuppgifter

Det är som huvudregel förbjudet att behandla känsliga personuppgifter om inte något undantag är tillämpligt.

4.4.1 Vad som kan vara känsliga uppgifter

Vissa personuppgifter är till sin natur särskilt känsliga och har därför ett starkare skydd. Det gäller exempelvis uppgifter som avslöjar en persons politiska åsikter, etniska ursprung, sexuella läggning och religion. Dessa kallas känsliga personuppgifter. En uppgift att någon är med i ett visst politiskt parti är ett exempel på en känslig personuppgift.

Exempel 18: CC uppger uttryckligen i sin profil på ett socialt medium att CC är medlem i det politiska partiet YY. Intresseorganisationen ÄÄ använder det sociala mediets inriktnings- och förstärkningstekniker för att rikta politisk reklam till användare som CC som är medlemmar i YY. Här agerar ÄÄ och det sociala mediet som gemensamt personuppgiftsansvariga. Eftersom de båda behandlar känsliga personuppgifter behöver båda utöver stöd i en rättslig grund ha stöd av något av undantagen från förbudet att behandla känsliga personuppgifter.

Det är även fråga om behandling av känsliga personuppgifter när den personuppgiftsansvariga gör antaganden eller drar slutsatser om hur en person kommer att rösta, till exempel eftersom personen har besökt en webbsida som förespråkar vissa politiska åsikter. Känsliga personuppgifter kan alltså skapas genom att dra slutsatser från och kombinera personuppgifter som till en början inte klassas som känsliga.

Exempel 19: Ett socialt medium använder aktivt uppgifter som DD tillhandahållit på sin profilsida på sociala medier om ålder, intressen och adress. Det sociala mediet kombinerar uppgifterna med observerade uppgifter om de webbplatser som DD besökt och DD:s ”gilla”-markeringar på det sociala mediet. Det sociala mediet använder uppgifterna och placerar DD i kategorin ”intresserade av vänsterliberal politik” för sitt erbjudande om inriktnings- och förstärkningstekniker och gör denna kategori tillgänglig för dem som vill betala för att använda sådana tekniker för att rikta budskap via mediet. Erbjudandet och användningen av kategorin ”intresserad av vänsterliberal politik” för att skicka reklam för sådana tekniker är en behandling av känsliga personuppgifter, eftersom kategorin enkelt skulle kunna användas för att rikta information till enskilda som har vänsterliberala politiska övertygelser. Genom att tilldela en användare en härledd politisk åskådning behandlar det sociala mediet känsliga personuppgifter.

Exempel 20: I DD:s profil på sociala medier avslöjas endast allmän information som namn och bostadsort, men en statusuppdatering visar att DD ofta deltar vid YY:s partimöten. Senare vill YY använda inriktnings- och förstärkningstekniker för att skicka politisk reklam till deltagare i mötena för att uppmuntra dem att ansluta sig till partiet. Om DD:s personuppgifter i statusuppdateringen behandlas för sådana ändamål utgör det enligt IMY:s bedömning en behandling av känsliga personuppgifter.

Det spelar ingen avgörande roll om slutsatser om känsliga personuppgifter är korrekta eller felaktiga.

Exempel 21: Partiet YY har utifrån observerade uppgifter dragit slutsatsen att CC sympatiserar med partiets politiska program och betalar en leverantör av beteendestyrda annonser på internet för att skicka politisk reklam till CC. Egentligen är CC dock en meningsmotståndare till partiet. Men även om uppgifterna är felaktiga har YY här behandlat känsliga personuppgifter om CC.

4.4.2 Vilka undantag som gör behandling av känsliga personuppgifter tillåten

Huvudregeln är att det är förbjudet att behandla känsliga personuppgifter, men det finns undantag. Den som behandlar känsliga personuppgifter behöver ha klart för sig att det finns stöd för behandlingen i något sådant undantag. Det finns flera undantag från förbudet att behandla känsliga personuppgifter, men här tar vi endast upp de undantag som typiskt sett kan vara aktuella vid politisk marknadsföring.

I exempel 18 ovan är till exempel förmodligen de enda möjliga undantag som kan vara aktuella att CC har lämnat ett uttryckligt samtycke eller tydligt själv har offentliggjort den känsliga personuppgiften om politiska åsikter.

4.4.2.1 Undantaget för uttryckligt samtycke

Ett undantag är om den som uppgifterna avser har lämnat sitt *uttryckliga samtycke*. Samtycket omfattar dock bara de ändamål som personen har godkänt.

Med ordet ”uttryckligt” i begreppet *uttryckligt samtycke* avses hur samtycket lämnas och innebär att enskilda avger en uttrycklig samtyckesförklaring. Ett uttryckligt samtycke kan ges skriftligen, till exempel genom undertecknande av en samtyckesförklaring. I digitala sammanhang kan det ske genom att fylla i ett elektroniskt formulär, skicka ett mejl, ladda upp ett skannat dokument med underskrift eller elektronisk underskrift. Teoretiskt sett kan även muntliga förklaringar vara tillräckligt uttryckliga, men det kan vara svårt att bevisa att samtliga villkor var samtycket var uppfyllda när samtyckesförklaringen lämnades.

Dubbel kontroll av samtycket kan vara ett sätt att kontrollera att det uttryckliga samtycket är giltigt.

Exempel 22 – dubbel kontroll: Partiet YY vill behandla uppgifter om DD:s politiska åsikter. YY informerar DD via mejl om att YY avser att behandla uppgiften. YY förklarar i mejlet att YY begär samtycke för att få använda uppgiften för ett

specifikt ändamål. Om DD samtycker till att uppgifterna används ska YY be DD svara genom ett mejl som innehåller orden ”Jag samtycker”. När DD skickat sitt svar får DD en verifieringslänk som DD måste klicka på, eller ett sms med en verifieringskod, för att bekräfta sitt samtycke.

4.4.2.2 Undantaget för tydligt offentliggjorda uppgifter

Ett annat undantag är om den som uppgifterna avser *på ett tydligt sätt själv har offentliggjort uppgifterna*. Ordet ”tydligt” innebär att tröskeln är hög för att detta undantag ska kunna åberopas. Vad som är avgörande är personens egen avsikt. Ett exempel på när en ensam omständighet är tillräckligt för att visa en sådan avsikt är när en person kandiderar för ett visst parti. I övrigt räcker en enstaka omständighet normalt inte för att visa en sådan avsikt. Relevanta faktorer för bedömning kan vara:

- Standardinställningarna på det sociala mediet (det vill säga om en användare har vidtagit särskilda åtgärder för att ändra dessa standardinställningar från privata till offentliga).
- Typ av socialt medium (det vill säga om syftet för användarna är att hålla kontakt med nära bekanta eller skapa intima relationer som på dejtingsajter), eller om mediet erbjuder ett bredare spektrum av kontakter som yrkesmässiga relationer, mikrobloggning, delning av media och recensioner med mera.
- Hur tillgänglig sidan där uppgifterna offentliggörs är (till exempel om informationen är allmänt tillgänglig eller om ett konto måste skapas för att få tillgång till den).
- Hur tydlig informationen om att ens personuppgifter på sajten kommer att bli offentliga är för användaren (det vill säga om det till exempel finns en kontinuerlig textruta med information om det på webbplatsen, eller om knappen för att publicera informationen informerar användaren om att den kommer att bli offentlig).
- Om den enskilde själv har offentliggjort uppgifterna eller om uppgifterna har offentliggjorts av en tredje part (till exempel ett foto som publicerats av en vän som avslöjar känsliga uppgifter) eller har härletts från andra uppgifter (till exempel kan detaljerade uppgifter om matvanor avslöja uppgifter om hälsa).

Nedan följer några exempel på tillämpning av dessa kriterier.

Exempel 23: CC är medlem i det politiska partiet YY och deltar i YY:s partimöte för att höra mer om deras tankar kring utvecklingen av landsbygden i CC:s hemkommun. Eftersom CC endast deltar i mötet har CC troligen inte haft som avsikt att offentliggöra att CC är medlem i partiet.

Exempel 24: När DD öppnade ett konto på en plattform för mikrobloggning på sociala medier fyllde DD i sin profil att DD är homosexuell. Eftersom DD är konservativ valde DD att gå med i konservativa grupper och fick information vid registreringen om att meddelanden som skickas via plattformen är offentliga. Ett konservativt politiskt parti vill använda sig av plattformens erbjudande för inriktnings- och förstärkningstekniker för att nå personer som har samma politiska tillhörighet och sexuella läggning som DD. Eftersom medlemmarnas sexuella

läggning automatiskt är privat och DD inte har vidtagit några åtgärder för att offentliggöra uppgiften har den inte offentliggjorts på ett tydligt sätt. Uppgiften får därför inte behandlas med stöd av undantaget.

4.4.2.3 Undantaget för behandling inom vissa ideella organisationer

Ett ytterligare undantag är när känsliga personuppgifter behandlas inom vissa ideella organisationer. En ideell organisation med politiskt syfte får behandla känsliga personuppgifter om nuvarande och tidigare medlemmar och andra personer som på grund av organisationens ändamål har regelbunden kontakt med organisationen. Undantaget gäller bara för känsliga personuppgifter för dessa personer. En viktig begränsning i undantaget är att uppgifterna inte utan de berördas samtycke får lämnas ut till en tredje part (till exempel en leverantör av sociala medier) för att rikta politisk reklam till dem eller för att hitta personer med liknande egenskaper att rikta sådan reklam till (så kallade lookalike-målgrupper).

Exempel 25: Det politiska ungdomsförbundet ZZ vill ladda upp sitt medlemsregister till en leverantör av ett socialt medium för att kunna skicka politisk marknadsföring till användare av det sociala mediet som liknar förbundets medlemmar. ZZ behöver få medlemmarnas samtycke för att undantaget ska kunna tillämpas och detta ska vara tillåtet, eftersom ZZ därigenom behandlar känsliga uppgifter (politisk åskådning) som lämnas ut till tredje part (leverantören av det sociala mediet).

4.5 Rätt till information och utövande av rättigheter

Ni behöver lämna klar och tydlig information om behandlingen till dem vars personuppgifter ni behandlar. Om ni använder inriktnings- och förstärkningstekniker bör ni informera väljarna om varför de får ett visst budskap, vem som är personuppgiftsansvarig och hur de kan utöva sina rättigheter. Informationen ska ges i en klar, tydlig, begriplig och lätt tillgänglig form.

Ni behöver också skapa rutiner för att hantera dessa personers begäranden om att få utöva sina rättigheter. Det gäller särskilt rättigheterna till tillgång, rättelse, radering och invändning. Tidpunkten för när en begäran kom in avgör vilka uppgifter som ni behöver ge tillgång till. Om någon har begärt tillgång får ni inte radera uppgifter för att slippa lämna ut dem om ni vid hantering av begäran upptäcker att behandlingen är olaglig.

Ni behöver underlätta för den registrerade att utöva sina rättigheter. Det innebär bland annat att inte ställa upp formkrav för hur begäranden får lämnas in. Det innebär även att ni inte får ha mer betungande krav för identifiering av den person som vill utöva sina rättigheter än vad som är proportionerligt och som gäller i andra, tidigare etablerade och verifierade kontaktvägar som ni har med som vill utöva sina rättigheter.

Enskilda har som huvudregel rätt att direkt till organisationer invända mot utskick som organisationerna gör för att främja sina mål och ideal. Detta torde även gälla politiska partier i sina valkampanjer, till exempel vid uppmaningar till väljare om att donera till eller stödja en valkampanj eller göra något, såsom att rösta på ett visst parti eller en viss kandidat.

4.6 Konsekvensbedömning kan krävas

En politisk aktör som vill använda inriktnings- och förstärkningstekniker i samband med en valkampanj behöver ta ställning till om en konsekvensbedömning avseende dataskydd behöver göras innan behandlingen påbörjas. Utöver vägledningen för denna bedömning på IMY:s webbplats finns IMY:s förteckning enligt artikel 35.4 i dataskyddsförordningen som innehåller kriterier och exempel på behandlingar som kräver att en konsekvensbedömning görs. Av förteckningen följer att en konsekvensbedömning behöver göras om antingen minst två av kriterierna finns med i den planerade behandlingen eller om behandlingen omfattas av något av exemplen.

Kriterier ur förteckningen som kan tänkas vara uppfyllda i samband med användning av inriktnings- och förstärkningstekniker är om ni:

- systematiskt övervakar människor, till exempel genom att samla in personuppgifter från internetanvändning i offentliga miljöer
- behandlar känsliga personuppgifter
- behandlar personuppgifter i stor omfattning och kombinerar personuppgifter från två eller flera behandlingar på ett sätt som skiljer sig från vad de registrerade rimligen kunnat förvänta sig, till exempel när register samkörs
- inhämtar uppgifter från sociala medier för att profilera fysiska personer och därefter riktar marknadsföring till vissa utvalda grupper.

Av listan med *exempel* på behandlingar som kräver att en konsekvensbedömning utförs framgår bland annat att en konsekvensbedömning behöver göras om ni inhämtar uppgifter från sociala medier för att profilera fysiska personer och därefter riktar marknadsföring till vissa utvalda grupper.

Exempel 26: Det politiska partiet YY vill uppmuntra användare av sociala medier att rösta på en viss politisk kandidat i det kommande valet. De vill rikta sig till äldre människor som bor på landsbygden, regelbundet går i kyrkan och inte har rest utomlands under de senaste två åren.

Det sociala mediet och YY har ett gemensamt personuppgiftsansvar för behandlingen, som utgörs av att matcha profilen med den politiska reklamen. Både YY och leverantören av det sociala mediet behöver bedöma om behandlingen kräver en konsekvensbedömning avseende dataskydd. De har båda tillräckliga kunskaper om de kriterier som används för riktad marknadsföring mot enskilda personer för att se att behandlingen sannolikt leder till en hög risk för registrerades grundläggande friheter och rättigheter samt att en konsekvensbedömning behöver utföras innan behandlingen påbörjas.

Om en konsekvensbedömning avseende dataskydd krävs bör det gemensamma arrangemanget mellan sociala mediet och YY behandla frågan hur de såsom gemensamt personuppgiftsansvariga bör genomföra konsekvensbedömningen och säkerställa att ett relevant kunskapsutbyte äger rum. Det sociala mediet är troligen bättre lämpad att bedöma viss behandling, eftersom YY endast väljer allmänna kriterier för att rikta sin reklam.

4.7 Överföring till tredjeland

Överföring av personuppgifter till tredjeland är som regel när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området.[1] Sådana överföringar är tillåtna under vissa förutsättningar.

Exempel på överföring av personuppgifter till tredjeland är när ni:

- anlitar ett personuppgiftbiträde i ett land utanför EU/EES
- ger någon utanför EU/EES tillgång, exempelvis läsbehörighet, till personuppgifter som finns lagrade inom EU/EES
- lagrar personuppgifter i en molntjänst som är baserad utanför EU/EES.

Att publicera något på internet är inte en tredjelandsöverföring om webbplatsen lagras hos en internetleverantör som är etablerad inom EU/EES.

Genom dataskyddsförordningen har alla EU:s medlemsstater ett likvärdigt skydd för personuppgifter och personlig integritet. Detta gäller även EES-länderna. Därför kan personuppgifter föras över fritt inom detta område utan begränsningar.

Utanför EU/EES däremot finns inga generella regler som ger motsvarande garantier. Dataskyddsförordningen innehåller därför regler om under vilka förutsättningar det är tillåtet att föra över personuppgifter till länder utanför EU/EES.

Under vissa förutsättningar är det tillåtet att överföra personuppgifter utanför EU/EES:

- det finns ett beslut från EU-kommissionen om att exempelvis ett visst land utanför EU/EES säkerställer så kallad adekvat skyddsnivå
- ni har vidtagit lämpliga skyddsåtgärder, till exempel bindande företagsbestämmelser eller standardavtalsklausuler.
- särskilda situationer och enstaka fall.

Om skyddsnivån i mottagarlandet inte är tillräcklig kan ni behöva vidta ytterligare skyddsåtgärder utöver till exempel standardavtalsklausuler. I vissa fall kan inga skyddsåtgärder kompensera för bristerna och göra överföringen tillåten. I sådana fall behöver ni avstå ifrån eller avbryta överföringen.[2]

5 Rättsinformation

- 1 kap. 1- 4 §§ Regeringsformen (RF)
- 1 kap. 11 § Yttrandefrihetsgrundlagen (YGL)
- Artikel 5-6
- Artikel 9
- Artikel 12-22

[1] EDPB har antagit riktlinjer 05/2021 om samspelet mellan artikel 3 (territoriellt tillämpningsområde) och kapitel V (tredjelandsöverföringar) i dataskyddsförordningen som bland annat innehåller en definition av begreppet ”överföring”. Dessa riktlinjer har varit ute på publik konsultation och ses nu över inför ett slutligt antagande.
[2] EDPB har antagit rekommendationer om när ytterligare skyddsåtgärder kan behövas och vad sådana åtgärder kan vara, se Rekommendationer 01/2020 om ytterligare åtgärder för att tillförsäkra att EU:s nivå av skydd för personuppgifter upprätthålls.

- Artikel 44-50
- Artikel 85

- Skäl 101-116
- Skäl 169

- Lagen (1998:527) om det statliga personadressregistret
- EDPB:s Uttalande 2/2019 om användningen av personuppgifter i samband med politiska kampanjer
- EDPB:s Guidelines 08/2020 on the targeting of social media users