SWEDMA

Svensk Branschkod för integritetsskydd vid marknadsföring

Fastställd den 18 november 2019
Version 1.1

Senast reviderad 1 december 2019

Syfte, omfattning och ändamål

Svensk Branschkod för integritetsskydd vid marknadsföring (Branschkoden) är ett konsoliderat dokument som ersätter de tidigare branschreglerna från 1998 ”*Regler för användning av personuppgifter m.m. vid direktmarknadsföring för försäljnings-, insamlings, medlemsvärvningsändamål och liknande*” samt ”*Etiska regler för adresserad direktreklam (ADR)*” respektive ”*Etiska regler för oadresserad direktreklam (ODR)*”, båda från 2012.

Branschkoden syftar till att säkerställa ett ansvarsfullt uppträdande inom det svenska näringslivet genom att ge erforderligt skydd för den personliga integriteten i samband med marknadsföring. Branschkoden omfattar marknadsföring riktad till konsumenter (B2C).

Branschkoden ska ge vägledning för integritetsskydd vid marknadsföring och behandling av personuppgifter för marknadsföringsändamål utifrån de krav som ställs. Branschkoden ska vidare främja en enhetlig tillämpning av dessa regler.

Branschkoden har tagits fram av branschorganisationen Swedish Data & Marketing Association (SWEDMA) med ca 250 medlemmar verksamma inom datadriven marknadsföring.

För efterlevnaden av Branschkoden svarar Etiska Nämnden för Direktmarknadsföring (DM-nämnden).

Branschkoden har fastställts genom beslut av styrelsen för SWEDMA. Koden revideras årligen samt vid behov.

Branschkoden är näringslivets tolkning av regelverket men det kan hända att respektive tillsynsmyndighet (Datainspektionen, Konsumentverket/KO eller Post- och Telestyrelsen) eller domstol i vissa fall kan göra en annan bedömning.

Branschkoden utgör god affärssed i Sverige.

Definitioner m.m.

Med *marknadsföring* avses alla åtgärder som en näringsidkare vidtar i syfte att öka sin avsättning. Det betyder t.ex. att alla framställningar (all kommunikation), oavsett medium, som har ett kommersiellt syfte och som har rent kommersiella förhållanden till ändamål utgör marknadsföring. Med syfte och förhållande menas vanligtvis framställningar om näringsidkarens affärsverksamhet eller däri tillhandahållna produkter. Avsändaren ska vara näringsidkare eller någon som agerar på dennes uppdrag.

I Branschkoden så omfattar begreppet marknadsföring dock inte kommunikation efter köp inkl. s.k. servicekommunikation som t.ex. beställningsbekräftelser, uppdaterade avtalsvillkor, att beställd vara finns för uthämtning, påminnelse om betalning eller påminnelse om att avtal inom kort upphör eller förlängs. Detta undantag ska dock tolkas snävt.

Icke-kommersiella meddelanden (t.ex. politiska budskap från politiska partier) utgör inte marknadsföring och omfattas således inte av Branschkoden.

Direktmarknadsföring finns inte närmare definierat i lagstiftningen. I Branschkoden förekommer två olika slags direktmarknadsföring; digital respektive analog.

Med digital direktmarknadsföring avses t.ex. e-post, SMS, MMS, push-notiser, "direktmeddelanden" i sociala medier (messenger) eller s.k. robotsamtal Däremot omfattas inte riktad annonsering (bannerannonsering) eller sponsrade inlägg i sociala medier.

Med analog direktmarknadsföring kommunikation som förmedlas genom fysiska handlingar (adresserad- respektive oadresserad brevlådereklam) eller telefonsamtal från fysisk person.

Begrepp som finns definierade i GDPR[1] som t.ex. *personuppgifter, känsliga personuppgifter, behandling, personuppgiftsansvarig, personuppgiftsbiträde, profilering m.fl.* har den innebörd som anges i GDPR.

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

1. Behandling av personuppgifter för marknadsföringsändamål

Allmänna principer

Vid all behandling av personuppgifter gäller enligt GDPR att behandlingen ska vara laglig, korrekt och öppen i förhållande till dem vars personuppgifter behandlas. Vidare får uppgifterna bara behandlas för de ändamål som angivits av den personuppgiftsansvarige. De uppgifter som behandlas får inte vara alltför omfattande i förhållande till ändamålet (uppgiftsminimering). Uppgifterna får inte sparas längre än nödvändigt och de ska behandlas som en värdehandling dvs. skyddas mot t.ex. otillåten eller obehörig åtkomst eller behandling. Att informera dem vars personuppgifter behandlas (öppenhet) är ett viktigt krav i GDPR. Det är också viktigt att veta att det den som är personuppgiftsansvarig som ska kunna visa (bevisa/dokumentera) sin rätt att använda personuppgifterna. Om flera parter är inblandade i behandlingen är det viktigt att rollerna klarläggs (personuppgiftsansvarig, personuppgiftsbiträde eller gemensamt personuppgiftsansvariga).

1.1 Insamling av personuppgifter m.m.

1.1.1 Bestämmande av ändamål

Du som företag måste specificera ändamålet med behandlingen/behandlingarna – varför du vill behandla personuppgifter. I Branschkoden är ändamålet marknadsföring.

Du kan normalt inte byta ändamål utan att informera den enskilde och, om du valt att basera behandlingen av personuppgifter på samtycke, måste du inhämta ett nytt samtycke för det nya ändamålet.

1.1.2 Laglig grund för behandling av personuppgifter

Innan ditt företag samlar in personuppgifter (påbörjar en behandling av dem) måste ni säkerställa att ni har en laglig grund för behandlingen.

Behandling av personuppgifter för marknadsföringsändamål kan normalt ske på tre grunder: fullgörande av avtal, berättigat intresse eller samtycke. För känsliga personuppgifter gäller dock som huvudregel ett krav på samtycke för behandling.

1.1.2.a Fullgörande av avtal

Den kommunikation med kund som krävs för att ditt företag ska kunna fullgöra sina åtagande i samband med köpet, det vill säga det avtal som ingåtts med kunden, har företaget rätt – och skyldighet – att fortsätta med. Fullgörande av avtal är laglig grund och inget samtycke krävs.

En kundklubb, ett lojalitetsprogram eller liknande utgör ett avtal mellan företaget och den enskilde. Behandling av personuppgifter som krävs enligt avtalet kan då baseras på den lagliga grunden fullgörande av avtal.

Marknadsföring som sker efter ett köp av en produkt och som inte baseras på avtalsförhållande, t.ex. utskick via e-post eller marketing automation, kan däremot inte baseras på denna grund.

1.1.2.b Berättigat intresse (intresseavvägning)

Berättigat intresse innebär att ändamålet för behandlingen av personuppgifterna ska ha betydelse för er affär. Argument som styrker behandlingens vikt för er affär måste dokumenteras.

Väljer du att använda berättigat intresse ska du göra ett ”balanstest”. I balanstestet kan t.ex. ingå ditt och den enskildes intressen (dennes rimliga förväntan), effekten av behandlingen för den enskilde (positiv och negativ), om det finns andra skyddsåtgärder (minimering, avidentifiering, möjligheten att tacka nej till e-post, tekniska och organisatoriska åtgärder för att säkerställa att endast behörig personal behandlar personuppgifterna). Du bör också tydligt visa och dokumentera att individens intressen är väl omhändertagna i och med att ditt företag arbetar i enlighet med marknadsföringslagen, tillämpar NIX, följer etiska regler, ger möjlighet att göra invändningar och så vidare.

Individens rätt att göra invändningar kan omhändertas via tydligt kommunicerade möjligheter för individen att avregistrera sig från kommunikation i de olika kanaler ditt företag använder sig av. Säkerställ och dokumentera därför att kunden tydligt informeras om sin rätt att göra invändningar (artikel 21.1), det vill säga tydliggör opt-out-möjligheten för de olika typer av kommunikation och kanaler ditt företag använder.

Att man kan använda sig av berättigat intresse som grund för personuppgiftsbehandlingen framgår bland annat av artikel 21.1. Här görs det tydligt att en individ ska ha rätt att göra invändningar mot behandling av hens personuppgifter för till exempel direktreklam (inklusive profilering kopplad till direktmarknadsföringen) och behandlingen ska då vanligtvis upphöra. Formuleringen “rätt att göra invändningar” (opt-out) innebär att det inte handlar om att återkalla samtycke. Formuleringen innebär således att inte heller kommunikation som inte är direkt kopplad till köpet kräver aktivt samtycke, så länge berättigat intresse (artikel 6.1.f) kan argumenteras.

För det fall den enskilde motsätter sig viss behandling som grundas på berättigat intresse (det kan t.ex. vara behandling för marknadsföring eller profilering) så ska behandlingen ifråga upphöra såvida du inte kan visa att ditt intresse väger tyngre. Det kan t.ex. vara fråga om att du behöver fortsätta behandlingen för att kunna ta tillvara ett rättsligt anspråk (ni tvistar). Om invändningen rör direktmarknadsföring så ska behandlingen upphöra.

1.1.2.c Samtycke

För att det ska föreligga ett giltigt samtycke krävs att det är en frivillig, specifik, informerad och otvetydig viljeyttring från individen. Det betyder att det inte är tillåtet med t.ex. förkryssade rutor eller att lägga in samtycket i avtalsvillkoren om inte behandlingen är en central del av avtalet.

Ett minimikrav för att viljeyttringen ska vara informerad är att:

- du informerar individen om din identitet,
- ändamålet med behandlingen du vill ha samtycke för,
- mottagare eller kategorier av mottagare,
- vilka slags data du kommer att behandla,
- rätten att återkalla samtycket,
- i det fall samtycket söks för automatiserat beslutsfattande ska det särskilt anges samt,
- om personuppgifterna kommer att föras utanför EU.

Det ska också vara lika lätt att återkalla samtycket som det var att lämna det. Såvida det inte angetts specifikt, eller följer av nationell lagstiftning, gäller samtycket tills det återkallas.

För viss typ av behandling, exempelvis för behandling av känsliga personuppgifter, krävs som huvudregel ett samtycke från individen.

1.1.3 Varifrån personuppgifter kan samlas in

Personuppgifter för marknadsföringsändamål kan samlas in direkt från individen själv eller från ett register eller annan källa.

Att personuppgifter får delas (säljas) vidare framgår av skillnaden i informationskraven mellan artiklarna 13 och 14. Det är alltså inte förbjudet att ”köpa” personuppgifter utan samtycke från individerna ifråga.

1.1.4 Hur personuppgifter kan samlas in (cookies/pixel m.m.)

Personuppgifter för marknadsföringsändamål kan samlas in t.ex. genom att individen själv anger sin e-postadress eller sitt telefonnummer på t.ex. ett webbformulär (manuell insamling).

För det fall uppgifterna samlas in automatiskt eller på elektronisk väg krävs i vissa fall ett samtycke från individen. Det gäller t.ex. genom användning av cookies, pixlar eller liknande trackers. Enligt lagen om elektronisk kommunikation får uppgifter lagras i eller hämtas från en abonnents eller användares terminalutrustning endast om abonnenten eller användaren får tillgång till tydlig information om ändamålet/ändamålen med behandlingen och samtycker till den/dem. Samtycket ska i likhet med vad som anges i avsnitt 1.1.2.c vara frivilligt och informerat.

Cookies som är nödvändiga för sidans funktion (funktionscookies) kräver inte samtycke.

Vid användning av cookies måste du alltid lämna information om kakans funktionstid (tiden den lagras) samt om tredje part får del av uppgifterna som samlas in med hjälp av kakan. Om de uppgifter som samlas in med hjälp av kakan utgör personuppgifter måste du dessutom lämna ytterligare information enligt GDPR (se punkten 1.2.1 nedan).

1.2 Information till den registrerade

Kravet på öppenhet i förhållande till individen innebär att du som företag är skyldig att självmant och utan föregående begäran från enskild lämna viss information till dem vars personuppgifter du behandlar (använder). Detta framgår av bl.a. artiklarna 13 och 14 i GDPR. Informationskravet gäller oavsett vilken laglig grund du använder dig av.

Informationen ska lämnas klart och tydligt åtskild från t.ex. allmänna avtalsvillkor. Informationen ska lämnas på ett enkelt och lättbegripligt språk där du som företag bör sträva efter att beskriva och förklara vad du gör och varför. Det kan t.ex. vara att ”för att vi ska kunna skicka relevanta erbjudanden till dig kommer vi att utgå från din köphistorik”.

Informationen bör normalt kunna lämnas i två skikt, det betyder alltså att du lämnar en sammanfattning av det du bedömer vara den viktigaste information och där länkar vidare till den fullständiga informationen. Du som företag ska säkerställa att konsumenten på ett enkelt sätt kan få informationen men det krävs inte att du säkerställer att denne verkligen läst alltihopa.

Säkerställ och dokumentera även att ni informerar era befintliga kunder om de uppdateringar av allmänna villkor och integritetspolicy som eventuellt gjorts och var de kan hitta dessa i sin helhet.

Det finns två olika informationskrav beroende på varifrån du samlat in personuppgifterna.

1.2.1 Information vid insamling direkt från den registrerade

Om du har samlat informationen direkt från individen, t.ex. genom användning av pixel/ cookie eller genom att konsumenten själv angett t.ex. e-postadress/telefonnummer så gäller informationskravet i artikel 13.

Det betyder att följande information ska lämnas i de fall (om och i den mån) individen inte redan förfogar över information (kan förväntas känna till det):

- Identitet och kontaktuppgifter för den personuppgiftsansvarige, till en företrädare (om det finns) samt till dataskyddsombudet (om det finns),
- Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den rättsliga grunden för behandlingen,
- Om den rättsliga grunden är intresseavvägning – varför du anser dig ha rätt att behandla personuppgifterna,
- Att individen har rätt att återkalla ett ev. samtycke utan att det påverkar att den tidigare behandlingen varit laglig,
- Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period,
- Förekomsten av automatiserat beslutsfattande, inbegripet profilering. Du ska på ett enkelt sätt förklara hur det går till och vad som blir följden (GDPR anger att det ska lämnas ”meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för individen”),
- Om du delar personuppgifterna med någon - mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna,
- Att det föreligger en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör individen eller att invända mot behandling samt rätten till dataportabilitet,
- Rätten att inge klagomål till en tillsynsmyndighet,
- Huruvida tillhandahållandet av personuppgifter är ett lagstadgat eller avtalsenligt krav (dvs. om individen är skyldig att lämna sina personuppgifter). Om kravet som är nödvändigt för att ingå ett avtal samt huruvida den registrerade är skyldig att tillhandahålla personuppgifterna och de möjliga följderna av att dessa inte lämnas samt,
- I de fall ni överför eller planerar att överföra personuppgifterna till ett tredjeland (utanför EU/EES) eller en internationell organisation ska ni informera om det samt om Kommissionen beslutat om adekvat skyddsnivå föreligger eller saknas samt (vid överföring enligt artiklarna 46, 47 eller 49.1 i GDPR) särskild information om lämpliga och passande skyddsåtgärder.

Byter ni syfte med behandlingen så ska ni informera om det nya syftet samt ytterligare information som är relevant i punkterna ovan (t.ex. lagringsperiod, den enskildes rättigheter, rätten att återkalla ett samtycke, huruvida den enskilde är skyldig att lämna personuppgifterna samt förekomsten av automatiskt beslutsfattande inklusive profilering).

Om behandlingen av personuppgifter för direktmarknadsföringsändamål (inkl. profilering) grundas på den lagliga grunden berättigat intresse så har konsumenten rätt att få information om att denne när som helst har rätt att invända mot behandlingen ifråga (inklusive den profilering i den utsträckning som denna har ett samband med direktmarknadsföringen ifråga). Informationen ska

lämnas senast vid den första kommunikationen på ett sätt som är klart, tydligt och klart åtskilt från eventuell annan information.

1.2.2 Information vid insamling från någon annan än den registrerade t.ex. vid registerköp

Om personuppgifterna inte har erhållits från individen utan, t.ex. genom inköp från offentlig källa eller från företagsregister så gäller informationskravet i artikel 14.

Informationen enligt artikel 14 ska lämnas inom en rimlig period efter det att du fått del av personuppgifterna, dock senast inom en månad. Enligt GDPR ska det ske med beaktande av ”de särskilda omständigheter under vilka personuppgifterna behandlas”.

Om du använder personuppgifterna för kommunikation med individen så ska informationen lämnas senast vid tidpunkten för den första kommunikationen med individen (men alltså aldrig senare än 30 dagar efter att du fått personuppgifterna).

Den information som ska lämnas (om och i den mån) individen inte redan förfogar över information (kan förväntas känna till det) är:

- Identitet och kontaktuppgifter för den personuppgiftsansvarige, till en företrädare (om det finns) samt till dataskyddsombudet (om det finns),
- Ändamålen med den behandling för vilken personuppgifterna är avsedda samt den lagliga grunden för behandlingen,
- De kategorier av personuppgifter som behandlingen gäller (t.ex. kontaktuppgifter eller identitetsuppgifter),
- Om du delar personuppgifterna med någon - mottagarna eller de kategorier av mottagare som ska ta del av personuppgifterna,
- Varifrån personuppgifterna kommer och huruvida de har sitt ursprung i allmänt tillgängliga källor,
- Om den rättsliga grunden är berättigat intresse – varför du anser dig ha rätt att behandla personuppgifterna,
- Att individen har rätt att återkalla ett ev. samtycke utan att det påverkar att den tidigare behandlingen varit laglig,
- Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period,
- Förekomsten av automatiserat beslutsfattande, inbegripet profilering. Du ska på ett enkelt sätt förklara hur det går till och vad som blir följden (GDPR anger att det ska lämnas ”meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för individen”),
- Att det föreligger en rätt att för individen att nyttja sina rättigheter enligt GDPR som t.ex. en rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter, eller begränsning av behandling som rör individen eller att invända mot behandling samt rätten till dataportabilitet,
- Rätten att inge klagomål till en tillsynsmyndighet (Datainspektionen) samt,
- I de fall ni överför eller planerar att överföra personuppgifterna till ett tredjeland (utanför EU/EES) eller en internationell organisation ska ni informera om det samt om Kommissionen beslutat om adekvat skyddsnivå föreligger eller saknas samt (vid överföring enligt artiklarna 46, 47 eller 49.1 i GDPR) särskild information om lämpliga och passande skyddsåtgärder.

Byter ni syfte med behandlingen så ska ni, **före** den nya behandlingen, informera om det nya syftet samt därutöver lämna informationen om:

- lagringsperiod,
- om den rättsliga grunden är intresseavvägning – varför du anser dig ha rätt att behandla personuppgifterna,
- den enskildes rättigheter ifråga om tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör individen eller att invända mot behandling samt rätten till dataportabilitet,
- rätten att inge klagomål till en tillsynsmyndighet,
- varifrån personuppgifterna kommer och huruvida de har sitt ursprung i allmänt tillgängliga källor samt,
- förekomsten av automatiserat beslutsfattande, inbegripet profilering. Du ska på ett enkelt sätt förklara hur det går till och vad som blir följden (GDPR anger att det ska lämnas ”meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för individen”).

Om behandlingen av personuppgifter för direktmarknadsföringsändamål (inkl. profilering) grundas på den lagliga grunden berättigat intresse så har konsumenten även rätt att få information om att denne när som helst har rätt att invända mot behandlingen ifråga (inklusive den profilering i den utsträckning som denna har ett samband med direktmarknadsföringen ifråga). Informationen ska lämnas senast vid den första kommunikationen på ett sätt som är klart, tydligt och klart åtskilt från eventuell annan information.

Enligt GDPR behöver information enligt artikel 14 **inte** lämnas om tillhandahållandet visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning, eller i den mån informationskraven om Identitet och kontaktuppgifter till dig, din företrädare eller ditt dataskyddsombud, om ändamålen samt den rättsliga grunden, om kategorier av personuppgifter, om mottagarna eller kategorier av mottagare samt om överföring till tredje land/internationell organisation sannolikt kommer att göra det omöjligt eller avsevärt försvårar uppfyllandet av målen med den behandlingen.

Det finns även ett undantag från informationskravet i GDPR om det finns stöd för det i unionsrätt eller nationell lagstiftning eller om personuppgifterna ska hållas konfidentiella till följd av tystnadsplikt enligt unionsrätten eller medlemsstaternas nationella rätt.

Det är i dagsläget svårt att närmare ange näs dessa undantag skulle vara tillämpliga. Det rekommenderas därför att undantaget används med försiktighet.

1.3 Användning, lagring och radering av personuppgifter m.m.

1.3.1 Korrekta personuppgifter

Den personuppgiftsansvarige är skyldig att fortlöpande hålla de personuppgifter som behandlas aktuella och kontrollera att dessa är relevanta för ändamålet med behandlingen. Personuppgifter som är inaktuella, felaktiga eller inte längre relevanta ska så snart som möjligt rättas eller raderas (utplånas).

1.3.2 Vilka personuppgifter som får behandlas

Utgångspunkten i GDPR är att de uppgifter som behandlas får inte vara alltför omfattande i förhållande till ändamålet (uppgiftsminimering). Det är du som företag som bestämmer ändamålet med behandlingen (marknadsföring). Det är också du som bestämmer vilka personuppgifter som du behöver behandla för att uppnå syftet (att skicka sådan marknadsföring som mottagaren uppfattar som relevant). Det innebär emellertid inte att du kan behandla vilka personuppgifter som helst eller i obegränsad mängd. Det är du som företag som måste kunna visa varför behandlingen är relevant. En enkel tumregel är "on a need to have basis only". Uppgifter som kan vara "nice to have" någon gång i framtiden bör du alltså radera.

Du måste vara medveten om att vissa uppgifter är känsliga och normalt kräver samtycke som laglig grund.

Exempel: Även om ett Apotek anser sig behöva behandla köphistoriken för att skicka relevanta erbjudanden så bör samtycke inhämtas om det av köphistoriken går att utläsa den enskildes olika hälsotillstånd.

1.3.3 Förbud mot fortsatt marknadsföring och kravet på interna spärrlistor

Om en individ anmäler direkt till ditt företag att vederbörande inte vill att du ska behandla hens personuppgifter för marknadsföring så måste du normalt upphöra med det. Du måste också säkerställa att du inte behandlar personuppgifterna för marknadsföringsändamål i framtiden. Det görs normalt genom att du har interna spärrlistor. Du kan alltså inte nöja dig med att hänvisa till t.ex. NIX eftersom konsumenten har rätt att välja bort just din reklam men fortfarande vilja ha konkurrenternas. Den lagliga grunden för spärrlistan bör kunna vara fullgörande av rättslig förpliktelse.

Behandlingen ska upphöra så snart som möjligt och senast inom sju dagar såvida inte särskilda skäl föreligger.

1.3.4 Profilering

Enkelt uttryckt innebär profilering att du försöker lära känna personerna i din databas (kundregister eller prospekts) för att den marknadsföring som du skickar ska vara relevant för mottagarna. Rätt utförd är profilering effektiv och uppskattad av mottagarna.

Definitionen av profilering i GDPR är betydligt mer långtgående än t.ex. kontaktuppgifter som adress och telefonnummer eller ålder. Det framgår vidare att profilering kan baseras på intresseavvägning så länge profileringen inte inkluderar automatiserat beslutsfattande.

Det finns således inget generellt krav på samtycke från dem som ”profileras”. Däremot är det viktigt att du berättar **att** du gör det, **varför** du gör det, **hur** det går till samt att de registrerade alltid har **rätt att säga nej** till ytterligare profilering.

Om individen väljer att invända mot fortsatt profilering måste du upphöra med det.

Det är också av betydelse hur eller varifrån du samlar in uppgifterna du använder i profileringen eller hur du arbetar med dem. Uppgifter från allmänna källor är offentliga och således mindre integritetskänsliga än om du samlar in uppgifter om surfhistorik på nätet. Likaså är det av betydelse om du endast jobbar med sannolikheter jämfört med om du med säkerhet kan tillskriva personen vissa intressen eller egenskaper.

Det krävs samtycke som laglig grund om profileringen innebär mer långtgående följder än att konsumenten får ta ställning till om denne vill köpa en produkt eller inte. Samtycke som laglig grund krävs även vid s.k. automatiserat beslutsfattande (beslutet görs uteslutande på maskinell väg t.ex. baserat på algoritmer). Ett exempel är då konsument ansöker online om lånelöfte för köp av bostad.

1.3.5 Hur länge får personuppgifterna sparas

Utgångspunkten i GDPR är att du inte får spara personuppgifter längre än nödvändigt. I och med att du som företag bestämmer vilka personuppgifter du behöver behandla så bestämmer du också hur länge du behöver dem. Behöver du inte längre en personuppgift enligt den enkla tumregeln ”need to have” så får du inte heller spara den. Det kan också vara så att du behöver en personuppgift för ett visst ändamål (t.ex. bokföring). Då får du endast använda personuppgiften till det – du får alltså inte använda den till andra ändamål som t.ex. marknadsföring.

Frågan hur länge du kan spara en personuppgift för marknadsföringsändamål kan också bero på vilken typ av produkt som marknadsförs. Sällanköpsvaror som t.ex. vitvaror eller möbler som har en längre livscykel motiverar att personuppgifterna kan sparas betydligt längre än t.ex. dagligvaror. Motsvarande gäller för tjänster eller andra immateriella produkter.

1.3.6 Hur ska personuppgifterna skyddas

Du ska betrakta personuppgifterna som en värdehandling som du fått låna. Det betyder att du ska skydda dem från t.ex. obehörig åtkomst eller spridning. Du kan t.ex. använda dig av tekniska lösningar, kryptering samt policys som reglerar vilka av företagets anställda som har tillgång till/rätt att använda vilka personuppgifter.

Anlitar du underleverantörer ska du säkerställa att de vidtar motsvarande åtgärder.

1.4. Överföring av personuppgifter

1.4.1 Överföring mellan företag

Det är enligt GDPR tillåtet att överföra personuppgifter mellan företag och att köpa personuppgifter (register). Det är viktigt och ett krav enligt GDPR att du informerar dem vars uppgifter du behandlar vilka mottagare eller kategorier av mottagare (t.ex. samarbetspartners) som du delar uppgifterna med.

Vid överföringar till personuppgiftsbiträden (t.ex. underleverantörer) så ska ni enligt GDPR ha ett avtal (personuppgiftsbiträdesavtal). Det är fortfarande du (som personuppgiftsansvarig) som är ytterst ansvarig för behandlingen (se mer under avsnitt 1.5.1).

I vissa fall kan det vara svårt att avgöra om ditt företag och er samarbetspartner är gemensamt personuppgiftsansvariga eller om ditt företag eller samarbetspartnern är personuppgiftsbiträde åt den andra parten. Som enkel huvudregel gäller att den som bestämmer ändamålet med behandlingen är personuppgiftsansvarig. Om båda parter har bestämmanderätt om över alla eller vissa av de behandlade personuppgifterna är ni normalt gemensamt ansvariga och får då istället avtala utifrån det.

1.4.2 Överföringar mellan länder

Det är enligt GDPR tillåtet att överföra personuppgifter inom EU/EES. Utanför EU/EES är det däremot som huvudregel förbjudet. Möjligheterna till undantag regleras i GDPR och du bör kontakta

tillsynsmyndigheten (Datainspektionen) om du är osäker på vad som gäller. Ett av dessa undantag är vid ett uttryckligt samtycke till detta från dem vars personuppgifter du överför. Innan du ber om samtycket ska du ha informerat om riskerna som är förknippade med tredjelandsöverföringen.

1.5 Individens rättigheter

1.5.1 Individens rätt till tillgång

Du som personuppgiftsansvarig är på förfrågan från individen skyldig att svara på fråga om personuppgifter som rör honom eller henne håller på att behandlas. Den personuppgiftsansvarige ska då också lämna följande information:

- Ändamålen med behandlingen,
- De kategorier av personuppgifter som behandlingen gäller,
- De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer,
- Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period,
- Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling,
- Rätten att inge klagomål till en tillsynsmyndighet (Data inspektionen),
- Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.
- Förekomsten av automatiserat beslutsfattande, inbegripet profilering enligt artikel 22.1 och 22.4, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den registrerade.

Om personuppgifterna överförs till ett tredjeland eller till en internationell organisation, har individen rätt till information om de lämpliga skyddsåtgärder som vidtagits vid överföringen.

Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling. För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.

1.5.2 Individens rätt till rättelse

Du som personuppgiftsansvarig är på begäran av individen skyldig att utan onödigt dröjsmål rätta felaktiga personuppgifter som rör individen. Individen har även rätt att komplettera ofullständiga personuppgifter.

1.5.3 Individens rätt till radering (”rätten att bli bortglömd”)

Du som personuppgiftsansvarig är på begäran av individen skyldig att utan onödigt dröjsmål radera individens personuppgifter om något av följande gäller:

- Personuppgifterna är inte längre nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats,

- Den registrerade återkallar det samtycke på vilket behandlingen grundar sig enligt artikel 6.1 a eller artikel 9.2 a och det finns inte någon annan rättslig grund för behandlingen,
- Den registrerade invänder mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre, eller den registrerade invänder mot behandlingen i enlighet med artikel 21.2,
- Personuppgifterna har behandlats på olagligt sätt,
- Personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse i unionsrätten eller i medlemsstaternas nationella rätt som den personuppgiftsansvarige omfattas av eller,
- Personuppgifterna har samlats in i samband med erbjudande av informationssamhällets tjänster, i de fall som avses i artikel 8.1.

Om du som personuppgiftsansvarig har offentliggjort personuppgifterna ska du underrätta de som i egenskap av personuppgiftsansvariga behandlar personuppgifterna om att den registrerade har begärt att de ska radera eventuella länkar till, eller kopior eller reproduktioner av dessa personuppgifter. Ni har rätt att väga in tillgänglig teknik och kostnaden för genomförandet vidta rimliga åtgärder.

Ovanstående gäller dock inte om behandlingen är nödvändig för att utöva rätten till yttrande- och informationsfrihet eller för att du som personuppgiftsansvarig ska kunna fastställa, göra gällande eller försvara rättsliga anspråk.

1.5.4 Individens rätt till begränsning av behandling

För ändamålet marknadsföring föreligger en generell skyldighet att avsluta behandlingen (eller del av behandlingen som t.ex. profilering) av personuppgifter för det ändamålet om individen ger uttryck för det. Det gäller även om behandlingen grundas på lagliga grunden samtycke, begäran bör då normalt uppfattas som ett återkallande av samtycket.

Om det kan anses motiverat får du som företag i samband med bekräftelse av att du mottagit begäran informera om dess konsekvenser (t.ex. att erbjudanden inte längre är personliga utan generiska). Du har dock inte rätt att fortsätta behandlingen utan erforderlig viljeyttring från individen (t.ex. ett samtycke eller ett nytt köp av produkt).

Om begäran tydligt avser en kanal som t.ex. SMS eller e-post får behandling för marknadsföring i övriga kanaler fortsätta.

1.5.5 Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling

Du som personuppgiftsansvarig ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som begärts av individen. Det gäller dock inte om det är omöjligt eller medför en oproportionellt stor ansträngning.

Du som personuppgiftsansvarig är skyldig att på begäran av individen informera denne om vilka dessa mottagare är.

1.5.6 Individens rätt till dataportabilitet

Förutsatt att behandlingens lagliga grund är samtycke och behandlingen sker automatiserat har individen som huvudregel rätt att få ut de personuppgifter som rör honom eller henne och som han

eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format. Individen har också rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits personuppgifterna hindrar detta.

Överföringen ska på begäran av individen ske direkt från en personuppgiftsansvarig till en annan när det är tekniskt möjligt.

1.5.6 Individens rätt att göra invändningar m.m.

Se avsnitt 1.3.3 respektive 1.3.4.

1.6 Ansvar

1.6.1 Ansvar hos dig som behandlar personuppgifter

Du som personuppgiftsansvarig har bevisbördan för att du har rätt att behandla uppgifterna, dvs du ska ha tänkt igenom, klargjort och tagit beslut samt dokumenterat detta så att du kan visa upp för en tillsynsmyndighet, individ eller domstol hur du tagit ditt beslut. Du ansvarar för att ditt företag vidtagit erforderliga säkerhetsåtgärder för skyddet av den enskildes personuppgifter. Det gäller även dig som är personuppgiftsbiträde. Som enkel huvudregel i GDPR faller ansvaret primärt på felande part oavsett om denne är personuppgiftsansvarig eller personuppgiftsbiträde. Det innebär att du som behandlar personuppgifter är ansvarig för att behandlingen följer gällande lagstiftning.

2. Obeställd digital direktreklam

2.1 Obeställd reklam m.m.

2.1.1 Huvudregeln - kravet på samtycke

I lagen anges ett förbud mot obeställd marknadsföring (reklam) genom användning av elektronisk post, telefax eller sådana uppringningsautomater eller andra liknande automatiska system för individuell kommunikation som inte betjänas av någon enskild såvida inte den fysiska personen har samtyckt till det på förhand.

Som huvudregel är det alltså inte tillåtet att skicka reklam till privatpersoner (konsumenter) via digital direktmarknadsföring utan att avsändaren på förhand har inhämtat mottagarens samtycke (opt-in).

2.1.2 Samtyckets utformning

För att det ska föreligga ett giltigt samtycke krävs att det är en frivillig, specifik, informerad och otvetydig viljeyttring från individen. Det betyder att det inte är tillåtet med t.ex. förbikryssade rutor eller att lägga in samtycket i avtalsvillkoren om inte behandlingen är en central del av avtalet.

Samtycket ska anges genom att man använder ett klart, tydligt och lättbegripligt språk som beskriver vad mottagaren samtycker till.

Ett minimikrav för att viljeyttringen ska vara informerad är att du informerar den enskilde om din identitet, vad du vill ha samtycke för, om även andra än ditt företag kommer att kommunicera med den enskilde samt rätten att återkalla samtycket.

Det ska också vara lika lätt att återkalla samtycket som det var att lämna det. Såvida det inte angetts specifikt, eller följer av nationell lagstiftning, gäller samtycket tills det återkallas.

2.1.3 Undantag i kundförhållanden (soft opt-in)

Som undantag från huvudregeln kan avsändaren använda sig av en s.k. soft opt-in. Det innebär att du får skicka digital direktreklam utan att du på förhand har inhämtat mottagarens samtycke.

För att du ska få göra det krävs att **samtliga** villkor nedan är uppfyllda:

1. Kontaktuppgiften (t.ex. e-postadress/telefonnummer) har samlats in från mottagaren själv i samband med försäljning av en vara eller tjänst från det avsändande företaget,
2. mottagaren har i samband med försäljning informerats om att kontaktuppgiften kan användas för marknadsföringsändamål och har erbjudits möjlighet att avstå framtida kontakt,
3. mottagaren är kund eller har varit kund inom de senaste 12 månaderna,
4. marknadsföringen avser egna likartade varor och tjänster.

2.1.4 Möjlighet att tacka nej till ytterligare kommunikation

I varje meddelande som skickas ska mottagaren ha möjlighet att på ett enkelt sätt avböja fortsatt kommunikation i den kanalen. Det görs t.ex. genom en giltig adress dit mottagaren kan sända en begäran om att reklamen ska upphöra, genom att svara på SMS eller genom att länka till inställning

för push-notiser i enheten (telefon/platta). Avregistreringen ska ske utan kostnad (bortsett från trafikkostnaden).

3. Obeställd analog direktreklam

3.1 Obeställd reklam m.m.

3.1.1 Huvudregeln – rätten att tacka nej

I lagtexten anges att det är det tillåtet att skicka eller lämna reklam till privatpersoner (konsumenter) så länge mottagaren inte tydligt har motsatt sig det (opt-out).

3.1.2 Adresserad direktreklam (ADR)

Förutsatt att de inte är beställda räknas som ADR

- personadresserade kommersiella meddelanden som sänds med vanlig betald post,
- kommersiella meddelanden som sänds med vanlig betald post som utan att vara personadresserade ändå anger en utdelningsadress (semiadresserad reklam).

Alla meddelanden som sänds som ADR skall vara markerade så att mottagaren – utan att behöva ta del av innehållet – med ett minimum av ansträngning kan identifiera utskicket som reklam. mottagaren ska t.ex. inte behöva öppna ett kuvert utan det ska framgå redan på kuvertets utsida.

Alla meddelanden som sänds ut som ADR skall innehålla uppgift om namnet på det företag vars produkter marknadsföringen samt avser en uppgift om hur mottagaren kan komma i kontakt med företaget.

ADR som sänds till konsumenter skall innehålla uppgift om adresskälla. Med adresskälla avses det företag eller register varifrån marknadsföraren hämtat mottagaradressen. Till uppgiften om adresskälla skall fogas uppgift om adress eller telefon till källan så att mottagaren kan kontakta denna. Uppgift om adresskälla behöver dock inte lämnas om marknadsföraren har anledning att anta att mottagaren inser varifrån adressen hämtats, t.ex. till följd av kundförhållande, medlemskap, eller liknande.

Om mottagaren tydligt motsatt sig att bli kontaktad genom ADR så ska avsändaren respektera det. Detta kan ske antingen genom att konsumenten direkt till avsändaren begär att denne inte ska kontakta konsumenten via ADR eller genom att konsumenten anmält sig själv och sin adress till Spärrtjänsten NIX adresserat.

I det första fallet så gäller begäran endast det enskilda företaget ifråga. Det innebär att konsumenten kan vara villig att ta emot ADR från andra företag som t.ex. konkurrenter. Det innebär att varje företag måste föra ett register över de personer som direkt till dem har anmält att de inte vill ha ADR.

Innan ADR sänds till konsumenter skall marknadsföraren undersöka huruvida adressatens namn finns i spärregistret NIX adresserat. Om adressatens namn finns i registret får ADR inte sändas till den personen. Om adressatens namn däremot inte finns i NIX adresserat får ADR sändas till personen under tre månader. Tiden räknas från datum för den version av NIX adresserat mot vilken kontrollen gjordes. Innan ADR sänds efter den tiden skall ny kontroll göras mot NIX adresserat.

I fråga om semiadresserade försändelser skall kontrollen avse den tilltänkte mottagaren. Om fler än en person är tilltänkta mottagare (t.ex. två föräldrar) bör kontrollen avse samtliga. I sådant fall bör försändelsen inte sändas om någon av mottagarnas namn/adress finns i NIX adresserat.

I följande fall får emellertid ADR sändas till konsumenter även om mottagarens namn finns i NIX adresserat:

- Konsumenten har lämnat sitt uttryckliga medgivande till att ADR sänds till honom eller henne,
- Det föreligger ett etablerat kundförhållande (ingånget avtal) mellan marknadsföraren och konsumenten. Detta undantag får tillämpas endast om erbjudandet avser samma typ av varor eller tjänster. Ett kundförhållande skall anses bestå även en tid efter det att avtalsförpliktelserna fullgjorts, men inte mer än ett år om inte särskilda skäl föreligger eller,
- Konsumenten har själv lämnat personuppgifter till marknadsföraren och därvid dels informerats om vilka kontaktvägar (brev, telefon, etc.) som marknadsföraren kan önska använda och dels givits möjlighet att avböja viss eller vissa kontaktvägar för marknadsföring.

3.1.3 Oadresserad direktreklam (ODR)

Med ODR menas reklam som utan att vara försedda med uppgifter om mottagarens namn eller adress delas ut direkt i mottagarens brevinkast/postlåda (inte skickad med posten).

Med ODR menas också reklam som är försedd med en utdelningsadress men ingen uppgift om mottagarens namn och som inte skickats med posten (även kallad fastighetsselekterad eller semiadresserad reklam).

Alla meddelanden som sänds som ODR skall vara markerade så att mottagaren – utan att behöva ta del av innehållet – med ett minimum av ansträngning kan identifiera utskicket som reklam. mottagaren ska t.ex. inte behöva öppna ett kuvert utan det ska framgå redan på kuvertets utsida.

Alla meddelanden som sänds ut som ODR skall innehålla uppgift om namnet på det företag vars produkter marknadsföringen samt avser en uppgift om hur mottagaren kan komma i kontakt med företaget.

ODR ska inte delas ut till hushåll på natten, dvs 22.00 – 06.00.

Vid utdelning av ODR ska reklamen helt stoppas in i brevinkastet så att den inte är synlig utifrån.

Om mottagaren tydligt motsatt sig att bli kontaktad genom ODR så ska avsändaren respektera det. Det sker genom att hushållet vid eller på sitt brevinkast satt upp en skylt/dekal eller liknande som visar att man tackar nej till reklam, en så kallad Nej-tack-skylt.

Budskapet ska vara klart och entydigt som t.ex. ”Ingen reklam, tack” och ”Reklam, nej tack” eller motsvarande.

Ytterligare budskap på skylten kan medföra att budskapet blir alltför otydligt och det räknas då inte som att mottagaren tydligt motsatt sig reklam.

Det strider även mot god sed att medvetet utforma ODR på ett sådant sätt att distributionen inte ska hindras av Nej-tack-skyltar.

Undantag från Nej-tack-skylt

Undantag för kravet på att undvika utdelning till hushåll med Nej-tack-skylt gäller för:

- icke-kommersiella meddelanden, till exempel information från myndigheter och annan samhällsinformation samt politisk information,
- periodisk skrift (gratistidningar/publikationer) med mer än en obetydlig mängd redaktionell

text och för vilken det finns ett utgivningsbevis samt,

- samproducerade delar av eller kommersiella bilagor till en periodisk skrift (enligt närmast föregående punkt) som har samma format eller papperskvalitet och som tydligt kan anses vara en del av den periodiska skriften.