Allmänna Dataskyddsförordningen

Sammanfattning

I detta PM redogörs för centrala delar kraven i EU:s allmänna Dataskyddsförordning ur en registeransvarigs t.ex. en kommun eller landstings/regions, ett personuppgiftsbiträdes och de registrerades synvinkel. Dataskyddsförordning (GDPR) innehåller 99 artiklar och 173 stycken s.k. skäl. Dataskyddsförordningen förkortas allmänt GDPR som står för General Data Protection Regulation (Dataskyddsförordningen).

Dataskyddsförordning blir tillämplig i Sverige den 25 maj 2018 och ersätter då personuppgiftslagen. GDPR utgör en ny generell reglering för behandling av personuppgifter inom EU. GDPR är direkt tillämplig och dess bestämmelser är tvingande. Nationell lagstiftning på området kommer endast kunna komplettera GDPR i den utsträckningen det är möjligt att göra undantag eller förtydliganden i förhållande till GDPR

GDPR ska tillämpas på behandlingen av personuppgifter både inom det offentliga och det privata. T.ex. har alla som har sina personuppgifter registrerade hos en kommun ett landsting/region rätt att få information om hur deras personuppgifter behandlas.

Dataskyddsförordningen

Europeiska unionens allmänna dataskyddsförordning (EU 679/2016) ska tillämpas inom hela EU från den 25 maj 2018. Förordningen tillämpas på behandlingen av personuppgifter både inom det offentliga och det privata. Den ersätter personuppgiftsdirektivet från 1995 och personuppgiftslagen (1998:204). Parallellt med GDPR utreds behovet av ytterligare flera nya lagar för nationella anpassningar av dataskyddet som ännu inte är beslutade.

Det övergripande syftet med GDPR är att säkerställa människors rätt till skydd av sina personuppgifter och därmed rätten till skydd för privatlivet. Ett annat mycket viktigt syfte är att fastställa regler för det fria flödet av personuppgifter inom EU och därmed lägga grund för en ökad digitalisering inom EU.

GDPR ger både den personuppgiftsansvarige och personuppgiftsbiträdet nya uppgifter och skyldigheter. Den registrerade får nya rättigheter. Grundläggande i GDPR är hur personuppgifter ska behandlas lagligt och när samt hur och av vem personuppgifter får behandlas.

Tillämpningsområde och definitioner

GDPRs tillämpningsområde (artikel 2 och 3)

GDPR ska tillämpas på automatisk behandling av personuppgifter. GDPR tillämpas också på annan behandling av personuppgifter när de personuppgifter som ska behandlas utgör en del av ett register.

GDPR ska tillämpas på behandlingen av personuppgifter inom ramen för den verksamhet som bedrivs av en organisation som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte. Vidare tillämpas GDPR också i vissa situationer på organisationer som är etablerade utanför unionen. GDPR ska tillämpas på exempelvis behandlingen av uppgifter om personer som befinner sig i unionen, om behandlingen har anknytning till utbjudande av varor eller tjänster till personerna eller anknytning till personernas beteende.

GDPR är inte tillämplig på fysiska personers behandling av personuppgifter som ett led i verksamhet som är helt och hållet privat eller saknar koppling till yrkes- eller affärsmässig verksamhet. Exempel på sådan privat verksamhet kan omfatta till innehav av adresser eller aktivitet i sociala nätverk i samband med sådan verksamhet.

GDPR är inte tillämplig på verksamhet som gäller nationell säkerhet. GDPR är inte tillämplig på EU:s medlemsstaters behandling av personuppgifter när de agerar inom ramen för unionens gemensamma utrikes- och säkerhetspolitik. GDPR är inte heller tillämplig på behandling av personuppgifter som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

Viktiga definitioner (artikel 4)

GDPR definierar personuppgift mer detaljerat än personuppgiftslagen och tar upp exempel på vilka uppgifter som definieras som personuppgifter.

Med personuppgift avses i GDPR varje upplysning som avser en identifierad eller identifierbar fysisk person. En identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett person- eller identifikationsnummer, en lokaliseringsuppgift eller online identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Enligt definitionen kan en personuppgift vara till exempel en lokaliseringsuppgift som säger någonting om en viss person; ett fotografi som i kombination med exempelvis adressuppgifter säger någonting om en viss person eller om personens levnadsförhållanden; eller en IP-adress som kan kopplas till en viss person; eller användarnamn.

Med behandling av personuppgifter avses åtgärder eller kombination av åtgärder som berör personuppgifter eller uppsättningar av personuppgifter, oberoende av om det utförs automatiserat eller inte, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning,

utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Ett personregister är en strukturerad samling av personuppgifter som är tillgängligt enligt särskilda kriterier. Datamängden kan vara centraliserad, decentraliserad eller spridd på bestämda grunder. Medlemsregister och användarregister är exempel på personregister.

Den personuppgiftsansvarige är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträdet är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Dataskydds principer (artikel 5)

I GDPR föreskrivs om principerna för behandling av personuppgifter. Syftet med principerna är att styra behandlingen av personuppgifter så att kraven i GDPR uppfylls och den registrerades rättigheter respekteras.

Enligt GDPR ska följande principer gälla vid behandling av personuppgifter:

1. Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade.

Med öppet sätt avses att det för de registrerade bör vara klart och tydligt hur uppgifter som gäller dem insamlas och används samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas. Öppenhetsprincipen kräver att all information och kommunikation i samband med behandlingen av personuppgifter är lättillgänglig och lättbegriplig.

2. Insamlingen av personuppgifter ska vara begränsad till ändamålet och ske för särskilda, uttryckligt angivna och berättigade ändamål. Uppgifterna får inte senare användas för ett ändamål som inte är bundet till ändamålet med de insamlade uppgifterna.

Det har ändå ansetts att om uppgifterna senare används för arkivändamål eller för historiska forskningsändamål eller statistiska ändamål gäller inte principen om ändamålsbegränsning.

3. Insamlingen av personuppgifter ska vara uppgiftsminimerad, dvs. inte för omfattande i förhållande till de ändamål för vilka uppgifterna behandlas, och uppgifterna ska vara adekvata och relevanta.

Personuppgifter bör behandlas endast om syftet med behandlingen inte rimligen kan uppnås genom andra medel.

4. Personuppgifterna ska vara korrekta och om nödvändigt uppdaterade. Den personuppgiftsansvarige ska med rimliga åtgärder säkerställa att personuppgifter som är inexakta och felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

Den personuppgiftsansvarige ska, till exempel med hjälp av fastställda tidsfrister, säkerställa att personuppgifter inte förvaras längre än nödvändigt.

5. Personuppgifter ska förvaras i en form som möjliggör identifiering av den registrerade endast under den tid som är nödvändig för de ändamål för vilka personuppgifterna behandlas. Uppgifter får dock förvaras längre, om de endast behandlas för arkivändamål av allmänt intresse, eller används för historiska forskningsändamål eller statistiska ändamål.

6. Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för uppgifterna och därmed uppgifternas integritet och konfidentialitet. Uppgifterna ska skyddas mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Då ska lämpliga tekniska eller organisatoriska åtgärder användas.

Laglig behandling av personuppgifter och dataskydds principer

Laglig behandling av personuppgifter (artikel 6)

Den personuppgiftsansvarige och personuppgiftsbiträdet får behandla personuppgifter endast på de grunder som framgår av GDPR. Enligt GDPR får personuppgifter behandlas om:

- den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål;
- behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås;
- behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige;
- behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person;
- behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning;
- behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

Den rättsliga grunden för behandling av personuppgifter enligt GDPR skiljer sig delvis från den i 8 § i personuppgiftslagen. Funktionellt sett motsvarar den rättsliga grunden i GDPR ändå i stor utsträckning den rättsliga grunden i personuppgiftslagen.

Uppgifter som gäller särskilda kategorier av personuppgifter ska i regel inte behandlas alls. Definitionen av särskild personuppgift i GDPR motsvarar med vissa ändringar personuppgiftslagens känsliga personuppgifter och omfattar uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt genetiska och biometriska uppgifter med vilka man entydigt kan identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Uppgifter som hör till särskilda kategorier av personuppgifter får behandlas om den grund som särskilt nämns i GDPR uppfylls. Särskilda personuppgifter får behandlas bland annat med personens uttryckliga samtycke, för att skydda personens grundläggande intressen eller då behandlingen är viktig för det allmänna intresset med stöd av lagstiftningen.

Om särskilda personuppgifter behandlas, ansvarar den personuppgiftsansvarige för att uppgifterna behandlas i enlighet med undantagsbestämmelsen i GDPR.

Ansvar

Enligt GDPR ska den personuppgiftsansvarige ansvara för att dessa principer och krav efterlevs. Dessutom ska den personuppgiftsansvarige kunna visa att principerna och kraven har efterlevts.

Den personuppgiftsansvarige ska se till att dataskyddsprinciperna efterlevs i alla stadier av behandlingen av personuppgifter. Den personuppgiftsansvarige ska i förväg bedöma vad principerna innebär i praktiken och hur de ska förverkligas i den egna verksamheten samt dokumentera denna bedömning.

Den personuppgiftsansvariges skyldigheter

Den personuppgiftsansvariges ansvar (artikel 24), inbyggt dataskydd och dataskydd som standard (artikel 25). Enligt GDPR ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och också i praktiken kunna visa att personuppgifterna behandlas i enlighet med GDPR.

Med tekniska och organisatoriska åtgärder avses exempelvis utbildning av personalen, interna anvisningar och föreskrifter, avtal och förbindelser om sekretess, övervakning av konton och användning, kryptering av uppgifter, anonymisering eller pseudonymisering av uppgifter, inspektion av datasystem och register, distansförbindelser, användningsövervakning, tekniska begränsningar, kontroll- och övervakningssystem, processer kring databokslut samt användning av uppförandekoder och certifikat.

Dessa åtgärder ska dimensioneras utifrån en riskbedömning, där man bland annat bör beakta behandlingens art, omfattning, sammanhang och ändamål samt de risker som gäller de registrerades rättigheter och friheter. Åtgärderna ska bedömas och ses över regelbundet och uppdateras vid behov.

Principen om inbyggt dataskydd och dataskydd som standard förutsätter att behoven och kraven i anslutning till dataskyddet identifieras och beaktas redan innan behandlingen inleds. I praktiken bör dessa behov utredas och slås fast redan när behandlingen av personuppgifter planeras, och exempelvis vid upphandling redan innan anbudsförfrågan görs, dvs. när man bestämmer funktionerna, processerna och systemens egenskaper. De datasystem där personuppgifter behandlas ska byggas upp så att de som standard genomför dataskyddsprinciperna och kraven i GDPR.

Enligt det i GDPR antagna riskbaserade förhållningssättet ställs de konkreta åtgärder som krävs i GDPR i förhållande till den risk som behandlingen av personuppgifter medför för den registrerades rättigheter och friheter. Den personuppgiftsansvarige ska omsorgsfullt bedöma riskerna i anslutning till behandlingen av personuppgifter och utifrån bedömningen slå fast de skyddsåtgärder som behövs och de övriga organisatoriska och tekniska åtgärder som ska motarbeta riskerna.

Med risk avses fysisk, materiell eller immateriell skada som eventuellt orsakas den registrerade av att personuppgifterna behandlas. Det kan till exempel ske när behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, social nackdel eller hävande av pseudonymisering. Risken kan vara större när man t.ex. behandlar uppgifter inom särskilda kategorier av personuppgifter, uppgifter om dem som är i en svagare ställning (t.ex. barn) eller när man behandlar stora mängder personuppgifter och behandlingen omfattar ett stort antal registrerade.

Register över behandling (artikel 30)

Den personuppgiftsansvarige, personuppgiftsbiträdet och deras företrädare ska föra ett skriftligt och elektroniskt register över all behandling av personuppgifter. Denna skyldighet gäller inte företag eller organisationer med färre än 250 anställda utom i det fall att den behandling som utförs sannolikt kommer att medföra en risk för registrerades rättigheter och friheter, behandlingen inte är tillfällig eller behandlingen omfattar särskilda kategorier av uppgifter (känsliga uppgifter).

Av registret över behandling ska bland annat framgå i sammanhanget viktig kontaktinformation, uppgiftsgrupper som behandlas och information om överföring av personuppgifter till tredjeländer. När de uppgifter som tillställs de registrerade (dvs. registerbeskrivningen, se nedan) är för externt bruk, utgör det här avsedda registret i första hand ett internt verktyg för den personuppgiftsansvarige, personuppgiftsbiträdet och deras företrädare.

Konsekvensbedömning och samråd (artikel 35 och 36)

Om behandlingen av personuppgifter sannolikt är förknippad med stora risker, ska den personuppgiftsansvarige göra en konsekvensbedömning av dataskyddet. Då bedöms riskerna i anslutning till behandlingen och också den personuppgiftsansvariges metoder att möta dessa risker. I GDPR finns närmare bestämmelser om riskbestämning och konsekvensbedömning.

En konsekvensbedömning ska göras särskilt om det används ny teknik eller om det gäller omfattande behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller särskilda kategorier av personuppgifter. En konsekvensbedömning ska också göras när det gäller en systematisk och omfattande bedömning som bygger på automatiserat beslutsfattande samt när det gäller systematisk övervakning av en allmän plats i stor omfattning.

Om konsekvensbedömningen visar att risken i anslutning till behandlingen är hög, och den personuppgiftsansvarige inte har vidtagit åtgärder för att minska risken, ska den personuppgiftsansvarige samråda med tillsynsmyndigheten innan behandlingen påbörjas (förhandssamråd). Förhandssamrådet ersätter anmälningsskyldigheten enligt personuppgiftslagen.

Dataskyddsombudets uppgifter (artikel 37, 38 och 39)

Alla myndigheter, dock inte är domstolarna i deras dömande verksamhet ska utse dataskyddsombud. Den privata sektorn är skyldig att utse dataskyddsombud och det gäller främst sådana privat aktörer vars kärnuppgifter är att behandla personuppgifter och då denna kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller vars kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av personuppgifter eller personuppgifter som rör fällande domar i brottmål och överträdelser.

GDPR har detaljerade bestämmelser om dataskyddsombudets ställning och uppgifter. Ett dataskyddsombud kan vara anställt i en verksamhet, eller utföra sina uppgifter på enligt ett tjänsteavtal. En koncern, fler myndigheter eller kommuner kan utse ett gemensamt dataskyddsombud.

Ett dataskyddsombud ska utses på grundval av sin yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd. Ett dataskyddsombud ska vara oberoende och får inte ta emot instruktioner som gäller utförandet av uppgifterna. Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå.

Ett dataskyddsombud får vid sidan av sina dataskyddsuppgifter utföra även andra uppgifter och uppdrag men dessa får inte leda till en intressekonflikt.

Dataskyddsombudet på ett ges möjlighet att delta hantering av alla frågor som rör dataskydd och behandling av personuppgifter. Enligt GDPR ska ombudet ges tillräckliga resurser och tillgång till personuppgifterna och behandlingsrutinerna. Ombudet har också rätt att få resurser för att upprätthålla sin sakkunskap.

Dataskyddsombudet får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter som dataskyddsombud.

Dataskyddsombudet ska informera och ge råd både till den personuppgiftsansvarige och till anställda i verksamheten när det gäller dataskydd och behandling av personuppgifter. Ombudet ska övervaka att GDPR efterlevs i organisationen, bygga upp medvetenheten om dataskydd och utbilda organisationens personal. Ombudet ska ge råd i fråga om konsekvensbedömningarna och samarbeta med tillsynsmyndigheten.

Överföring av personuppgifter till tredjeländer (kapitel V)

Personuppgifter får överföras till länder utanför EES-området endast om den personuppgiftsansvarige och personuppgiftsbiträdet uppfyller villkoren i GDPR. Överföring av personuppgifter till tredjeländer sker t.ex. när molntjänster används. Molntjänsterna kan använda servrar som finns utanför EES-området. Dessa kan även innehas av företag som finns utanför EES-området. I båda fallen ska överföringen av personuppgifter via molntjänster ske enligt reglerna om tredjeländer i GDPR.

Personuppgifter får överföras till ett tredjeland utan särskilt tillstånd, om kommissionen har beslutat att det tredje landet i fråga säkerställer en adekvat skyddsnivå (överföring på grundval av ett beslut om adekvat skyddsnivå). Kommissionen ska i Europeiska unionens officiella tidning och på sin webbplats offentliggöra en förteckning över de tredjeländer för vilka den har fastställt att skyddsnivån är eller inte längre är säkerställd.

Personuppgifter får även överföras till tredjeland efter att den personuppgiftsansvarige eller personuppgiftsbiträdet har vidtagit lämpliga skyddsåtgärder, och på villkor att de registrerade har tillgång till verkställbara rättigheter och effektiva rättsmedel. GDPR innehåller närmare bestämmelser om eventuella skyddsåtgärder och nämner bland annat avtal mellan myndigheter, bindande bestämmelser, kommissionens standardiserade bestämmelser, godkända certifieringsmekanismer och administrativa bestämmelser. Dessutom har GDPR bestämmelser för särskilda situationer.

För närvarande överförs personuppgifter till USA genom ett dataskyddsavtal kallat Privacy Shield, som kommissionen godkänt. I avtalet godkänns enskilda företag som trygga amerikanska företag och trygga mottagare av överförda personuppgifter.

Den registrerades rättigheter

Öppen information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter (artikel 12).

Den personuppgiftsansvarige ska planera sin verksamhet så att den registrerade på begäran kan få information som gäller behandlingen av personuppgifterna. Enligt GDPR ska informationen kunna presenteras i en koncis, klar och tydlig, begriplig och lätt tillgänglig form.

Den information som avses i artikeln är registren över behandling; de uppgifter som är föremål för granskning; information om rättelse, radering, begränsning, överföring av personuppgifter; information om invändningar mot behandling eller profilering samt anmälan om datasäkerhetsincidenter.

Informationen ska i regel tillhandahållas skriftligt. Om den registrerade lämnar begäran i elektronisk form, ska informationen i regel också tillhandahållas i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på ett tillförlitligt sätt.

Det finns tidsfrister för informationen till och åtgärderna angående den registrerade. Informationen ska ges utan onödigt dröjsmål och senast en månad efter att begäran togs emot. Det finns möjlighet till förlängning av tidsfristen på vissa villkor.

Information och den personuppgiftsansvariges åtgärder för utövandet av den registrerades rättigheter ska i regel tillhandahållas kostnadsfritt när det sker på den registrerades begäran.

Den personuppgiftsansvarige kan få ta ut en rimlig avgift för sina åtgärder eller vägra att tillmötesgå begäran, om den registrerades begäran är uppenbart ogrundad eller orimlig. Enligt GDPR kan en begäran anses orimlig till exempel då den registrerade upprepade gånger begär information uppenbart ogrundat. Det åligger den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller orimlig.

Information som ska tillhandahållas, dvs. register över behandling (artikel 13 och 14)

I GDPR finns en ingående beskrivning av den information som den personuppgiftsansvarige, när personuppgifterna erhålls, ska lämna till den registrerade. I praktiken är det fråga om ett register över behandling eller en liknande dokumentation, som dock har ett mer omfattande innehåll än registerbeskrivningarna enligt den nuvarande personuppgiftslagen.

I artikel 13 ingår en förteckning över information som ska lämnas till den registrerade, om personuppgifterna samlas in från den registrerade. I artikel 14 ingår en förteckning över information som den registrerade ska förses med, om personuppgifterna inte har erhållits från den registrerade. Informationen ska lämnas till den registrerade, om inte någonting annat följer av GDPR. Informationen behöver inte ges exempelvis om den registrerade redan förfogar över informationen eller om informationen är sekretessbelagd. Informationen behöver inte heller ges om tillhandahållandet av sådan information visar sig vara omöjligt eller skulle medföra en oproportionell ansträngning.

Om personuppgifterna erhålls av den registrerade, ska informationen till den registrerade ges när personuppgifterna samlas in. Om personuppgifterna erhålls från någon annan källa, ska den personuppgiftsansvarige ge den i GDPR uppräknade informationen till den registrerade inom rimlig tid, men senast inom en månad.

Den registrerades rätt till tillgång (artikel 15)

Den registrerade har rätt att med rimliga mellanrum få tillgång till de personuppgifter som har samlats in om honom eller henne samt till information som gäller behandlingen av personuppgifterna. ”Rimliga mellanrum” definieras inte närmare i GDPR. Alla registrerade bör därför ha rätt att få kännedom och underrättelse om framför allt orsaken till att personuppgifterna behandlas, under vilken tidsperiod behandlingen pågår, vilka som mottar personuppgifterna, logiken bakom automatisk behandling av personuppgifterna och konsekvenserna av sådan behandling. Dessutom har de registrerade rätt att få kännedom om sina rättigheter i förhållande till den personuppgiftsansvarige.

Den personuppgiftsansvarige ska på begäran meddela om denne behandlar personuppgifter om den som frågar. Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling, om det inte finns laga grund till att inte ge ut uppgifterna.

Den registrerades rätt att få tillgång till sina personuppgifter gäller också åtgärderna under behandlingen av dem (vem har behandlat, vilka uppgifter, när).

Den begärda informationen ska i första hand ges i elektronisk form. Enligt GDPR bör den personuppgiftsansvarige vidta alla rimliga åtgärder för att kontrollera identiteten på en registrerad som begär tillgång, särskilt inom ramen för nättjänster och i fråga om nätidentifierare. Den personuppgiftsansvarige ska genom ett riskbaserat förhållningssätt bedöma på vilket sätt identiteten hos den som frågar ska säkerställas och på vilket sätt informationen ska ges elektroniskt.

Rätt till rättelse (artikel 16)

Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få bristfälliga och felaktiga personuppgifter som rör honom eller henne rättade. Med beaktande av ändamålet med behandlingen, ska den registrerade ha rätt att komplettera ofullständiga personuppgifter, till exempel genom att lämna ett kompletterande utlåtande till den personuppgiftsansvarige.

En vidare lagring av personuppgifterna bör dock vara laglig, om detta krävs för att utöva yttrandefrihet och informationsfrihet, för att uppfylla en rättslig förpliktelse, för att utföra en uppgift i av allmänt intresse eller som ett led i myndighetsutövning som anförtrotts den personuppgiftsansvarige, med anledning av ett allmänt intresse inom

folkhälsoområdet, för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål eller för fastställande, utövande eller försvar av rättsliga anspråk.

Anmälningsskyldighet avseende rättelse eller radering av personuppgifter och begränsning av behandling (artikel 19)

Enligt GDPR ska den personuppgiftsansvarige underrätta var och en till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifterna eller begränsningar av behandlingen, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Likaså ska den personuppgiftsansvarige på begäran underrätta den registrerade om till vem uppgifter har lämnats ut.

Enligt GDPR ska den personuppgiftsansvarige underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska vidare informera den registrerade om dessa mottagare på den registrerades begäran.

Rätt till dataportabilitet (artikel 20)

Om den rättsliga grunden till behandlingen av personuppgifter är ett samtycke eller verkställande av ett avtal och behandlingen sker automatiskt, ska den registrerade ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har lämnat till den personuppgiftsansvarige. Uppgifterna ska lämnas i ett strukturerat, allmänt använt och maskinläsbart format. Den registrerade ska ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att den personuppgiftsansvarige som har personuppgifterna hindrar detta.

När den registrerade utövar sin rätt till dataportabilitet ska han eller hon ha rätt till överföring av personuppgifterna direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt.

I allmänhet betyder maskinläsbart format till exempel att den registrerade får en länk till sina personuppgifter.

Rätt att göra invändningar och automatiserat individuellt beslutsfattande, inbegripet profilering (artikel 21 och 22)

Den registrerade har rätt att motsätta sig behandling i direktmarknadssyfte och i en del andra situationer som nämns i GDPR, och då får hans eller hennes personuppgifter inte längre behandlas i syftena i fråga.

GDPR förbjuder inte profilering helt och hållet. Utgångspunkten är ändå att den registrerade ska ha rätt att inte bli föremål för profilering.

Anmälan av en personuppgiftsincident (artikel 33)

Den personuppgiftsansvarige har skyldighet att anmäla säkerhetsincidenter till tillsynsmyndigheten (Datainspektionen) och till de registrerade. Med personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

Den personuppgiftsansvarige ska anmäla en säkerhetsincident till tillsynsmyndigheten om möjligt inom 72 timmar efter att ha fått vetskap om den. Det gäller oberoende av om incidenten skett i den egna eller personuppgiftsbiträdets verksamhet. Den personuppgiftsansvarige kan låta bli att anmäla en säkerhetsincident endast om det är osannolikt att incidenten medför en risk för fysiska personers rättigheter och friheter.

Personuppgiftsbiträdet ska anmäla en säkerhetsincident till den personuppgifts-ansvarige utan onödigt dröjsmål efter att ha fått vetskap om den.

Om en personuppgiftsincident sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige också informera de registrerade om säkerhetsincidenten. I GDPR föreskrivs närmare om vad informationen till de registrerade ska innehålla.

Personuppgiftsbiträds avtal

I artikel 28 i GDPR sägs att när uppgifter behandlas av ett personuppgiftsbiträde ska hanteringen regleras genom ett avtal. I avtalet fastställs bland annat föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade samt den personuppgiftsansvariges skyldigheter och rättigheter.

GDPR föreskriver också tydligt vilken roll personuppgiftsbiträdet har, och de skyldigheter som biträdet (registerföraren) ges direkt i lagstiftningen har preciserats i förhållande till bestämmelserna i personuppgiftslagen. Enligt GDPR får personuppgiftsbiträdet till exempel inte anlita egna underleverantörer utan att ha fått ett särskilt eller allmänt skriftligt förhandstillstånd av den personuppgiftsansvarige (artikel 28.2).

Den personuppgiftsansvarige får endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i GDPR. Exempelvis vid anbudsförfarande ska man vid valet av leverantör fästa uppmärksamhet vid leverantörens möjligheter att uppfylla dataskyddskraven i GDPR och de dataskyddskrav som den personuppgiftsansvarige ställer.

Kravet på inbyggt dataskydd och dataskydd som standard påverkar också avtalen. Den personuppgiftsansvarige ska bestämma vilka praktiska krav som gäller i den egna personuppgiftsverksamheten. Villkor om hur kraven ska genomföras ska tas med i avtalen.

Avtal som direkt eller indirekt gäller behandling av personuppgifter ska omvärderas utgående från ändringarna i GDPR. Det kan till exempel vara fråga om avtal om utläggning av tjänster i anslutning till personer; avtal om köp av tjänster i anslutning till personer; avtal om datasystem som behandlar personuppgifter; eller direkta avtal om behandling av personuppgifter med en annan instans.

Påföljder och administrativa sanktioner

Rätt till ersättning (artikel 82)

Enligt GDPR ska varje person som har lidit skada till följd av en överträdelse av GDPR ha rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den uppkomna skadan. I första hand har den personuppgiftsansvarige det primära ansvaret och personuppgiftsbiträdet det sekundära. Ett personuppgiftsbiträde ska ansvara för skada endast om denne inte har fullgjort de skyldigheter i GDPR som specifikt riktar sig till personuppgiftsbiträden eller agerat utanför eller i strid med den personuppgiftsansvariges lagenliga anvisningar.

Administrativa sanktionsavgifter (artikel 83)

Utöver ersättning till den registrerade kan den personuppgiftsansvarige och personuppgiftsbiträdet bli tvungna att betala administrativa sanktionsavgifter på grundval av överträdelse av GDPR. En administrativ sanktionsavgift kan uppgå till högst 20 000 000 euro eller, om det gäller ett företag, utgöra 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst.

Beslut om påförande av administrativa sanktioner fattas av den tillsynsmyndighet som tillsatts med stöd av GDPR.

Enligt artikel 58.2 får varje medlemsstat fastställa regler för om och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga myndigheter och organ som är inrättade i medlemsstaten. Den kommande dataskyddslagen tas ställning till hur och vilka administrativa sanktioner som ska tillämpas på myndighetens verksamhet.

Parallellt med eller i stället för administrativa sanktioner kan tillsynsmyndigheten använda flera andra metoder att styra personuppgiftsansvariga samt få en lagstridig behandling att upphöra.

Det kan till exempel vara fråga om att utfärda reprimander eller varningar till den personuppgiftsansvarige, förelägga att behandlingen ska motsvara lagen inom en viss

tid, förelägga att den lagstridiga situationen rättas eller att felaktiga uppgifter rättas, uppställa behandlingsbegränsningar samt förelägga att dataöverföringar avbryts till en mottagare i ett tredjeland.