Bromölla kommun

KOMMUNAL FÖRFATTNINGSSAMLING **Nr 131.10**

Antagen/Senast ändrad	**Gäller från**	**Dnr**
Ks 2020-05-27 § 123	2020-05-28	2020/249

RIKTLINJER FÖR HANTERING AV PERSONUPPGIFTER

Riktlinjer för hantering av personuppgifter i Bromölla kommun

Innehåll

1 Inledning

Från och med den 25 maj 2018 gäller EU:s dataskyddsförordning (679/2016), även kallad GDPR (engelskans General Data Protection Regulation), för behandling av personuppgifter. Personuppgiftslagen (1998:204), även kallad PuL, har upphört att gälla.

Ett av syftena med dataskyddsförordningen är att skydda enskildas grundläggande friheter och rättigheter, särskilt deras rätt till skydd av personuppgifter. Ett annat syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras.

1.1 Vad är en behandling?

Med behandling avses en åtgärd eller en kombination av åtgärder rörande personuppgifter eller uppsättningar av personuppgifter, vare sig det sker på automatisk väg eller inte (artikel 4, GDPR).

Det gäller till exempel:

- Att sammanställa en lista med personuppgifter.
- Att ha elevadministration i kommunens IT-system.
- Att hantera e-post i kommunen.

Insamling, registrering, organisering, strukturering, lagring, bearbetning, ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering, sammanförande, begränsning, radering och förstöring är exempel på behandlingar enligt artikel 4, GDPR.

1.2 Vad är en personuppgift?

Med personuppgift avses all slags information som direkt eller indirekt kan härledas till en fysisk person som är i livet (artikel 4, GDPR).

Det gäller till exempel:

- Ett namn.
- Ett identifikationsnummer (personnummer, kundnummer etcetera).
- En lokaliseringsuppgift (bostadsadress, GPS-information etcetera).
- En online-identifikator (IP-nummer etcetera).
- Bilder, filmer, ljudupptagning etcetera.

Personuppgifter är vidare en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet (artikel 4, GDPR).

1.3 Vad räknas som känsliga personuppgifter?

Till känsliga personuppgifter räknas personuppgifter som avslöjar ras[1] eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa, uppgifter om en fysisk persons sexualliv eller sexuella läggning samt medlemskap i fackförening (artikel 9, GDPR).

Det finns flera andra typer av personuppgifter som är särskilt skyddsvärda. Datainspektionen kallar sådana uppgifter för integritetskänsliga personuppgifter.

Exempel på integritetskänsliga personuppgifter enligt Datainspektionen är löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter (till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler), information som rör någons privata sfär samt uppgifter om sociala förhållanden.

Enligt Datainspektionen har Sverige valt att ha ett särskilt skydd för personnummer och för de samordningsnummer som man kan få om man inte är folkbokförd i Sverige.

1.4 Strukturerat och ostrukturerat material

Dataskyddsförordningen gäller både strukturerat och ostrukturerat material.

Strukturerat material är sådana uppgifter som behandlas i dataregister, databaser samt ärende- och dokumenthanteringssystem. Det strukturerade materialet är byggt för att vara sökbart.

Ostrukturerat material är exempelvis bild och ljud. Det ostrukturerade materialet saknar i stort en uppbar sökfunktion.

1.5 Personuppgiftsansvarig (PuA)

Bromölla kommuns samtliga nämnder och styrelser, samt för organisationer där Bromölla kommun har rättsligt bestämmande inflytande, är personuppgiftsansvariga för sina respektive verksamhetsområden. Ansvaret innebär en yttersta skyldighet att tillse att gällande lagstiftning efterlevs.

Det handlar bland annat om att:

- Utse dataskyddsombud.
- Säkerställa att det finns tekniska och organisatoriska förutsättning att behandla personuppgifter med erforderlig säkerhet.
- Föra register över behandlingar av personuppgifter.
- Fastställa ändamål och syfte med behandling av personuppgifter, innan behandling påbörjas.
- Kunna visa att kraven i dataskyddsförordningen efterlevs genom dokumentation.

[1] I svensk lagstiftning används inte begreppet ras. I dataskyddsförordningen används dock begreppet, varför det är återgivet här.

Den personuppgiftsansvarige kan bli skadeståndsskyldig om överträdelse av dataskyddsförordningen sker.

1.6 Personuppgiftsbiträde (PuB)

Ett personuppgiftsbiträde är någon som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Det kan vara ett företag, en myndighet eller någon annan organisationsform. Den personuppgiftsansvarige får bara anlita biträden som ger tillräckliga garantier om att upprätthålla lämplig teknisk och organisatorisk säkerhet i enlighet med gällande krav.

1.7 Personuppgiftsbiträdesavtal (PuB-avtal)

Personuppgiftsbiträdets behandling av personuppgifter ska regleras i ett personuppgiftsbiträdesavtal (PuB-avtal) mellan personuppgiftsbiträdet (PuB) och personuppgiftsansvarig (PuA).

Kommunalförbundet Sydarkivera rekommenderar att SKR (Sveriges kommuner och regioner)s mallar och underlag används.

1.8 Bromölla kommun har ansvarsskyldighet

Bromölla kommun har ett övergripande ansvar att inte bara följa dataskyddsförordningen utan även att kunna visa hur detta görs.
I dataskyddsförordningen kallas det för ansvarsskyldighet (artikel 5 GDPR).

1.9 Dataskyddsombud (DSO)

Enligt dataskyddsförordningen (artiklarna 37-39 GDPR) ska den personuppgiftsansvarige utse ett dataskyddsombud (DSO) och anmäla det till tillsynsmyndigheten (se punkt 1.10).

Dataskyddsombudets huvudsakliga uppgift är att se till att kommunen följer dataskyddsförordningen. Dataskyddsombudet har dock inget ansvar för att den personuppgiftsansvarige följer förordningen. Det ansvaret ligger alltid hos den personuppgiftsansvarige.

Bromölla kommun är ansluten till tjänsten Gemensamt dataskyddsombud som utgörs av dataskyddsteamet inom kommunalförbundet Sydarkivera.

Exempel på vad Sydarkivera ska tillhandahålla genom avtalet:

- Råd och stöd till de personuppgiftsansvariga och dess anställda om skyldigheter enligt dataskyddsförordningen och annan dataskyddslagstiftning. Det kan till exempel vara rådgivning vid risk- och konsekvensbedömningar avseende dataskydd, vid upphandling av system eller applikationer som rör personuppgifter, vid ingående av personuppgiftsbiträdesavtal samt vid personuppgiftsincident.
- Utbildning i dataskyddsförordningen och annan dataskyddslagstiftning.
- Nätverksträffar för dataskyddssamordnare.

- Mallar för styrdokument, handledningar, informationstexter och liknande dokument för behandling av personuppgifter. Sydarkivera ska bjuda in till dataskyddsarbetsdagar minst två gånger per år för att arbeta med innehållet i mallarna och hålla dem uppdaterade.
- Övervakning av efterlevnad av dataskyddsförordningen och annan dataskyddslagstiftning via tillsyn hos den personuppgiftsansvarige.

Enligt avtalet med Sydarkivera har personuppgiftsansvarig följande ansvar:

- Utse dataskyddssamordnare som leder det lokala dataskyddsarbetet och som är kontaktperson gentemot Sydarkivera. Vidare är det också dataskyddssamordnaren som rapporterar till sin förvaltningsledning i samråd med Sydarkivera.
- Fastställa en lokalt anpassad organisation för dataskyddsarbetet med råd och stöd från Sydarkivera. Det är den lokala organisationen som ska utföra det operativa arbetet på plats hos personuppgiftsansvarig, till exempel inventera personuppgiftsbehandlingar, vid behov processkartlägga sin organisation, lämna ut registerutdrag, föra register över behandlingar, ta fram lokalt anpassade dokument utifrån tillhandhållna mallar och som gör risk- och konsekvensbedömningar avseende dataskydd.
- När risk- och konsekvensbedömningar avseende dataskydd görs ska dataskyddsombudet (Sydarkivera) rådfrågas enligt artikel 35 GDPR.
- Fastställa interna riktlinjer och policydokument för behandling av personuppgifter samt andra dokument som rör behandling av personuppgifter med råd och stöd från Sydarkivera.

1.10 Tillsynsmyndighet

Enligt dataskyddsförordningen (artiklarna 51-59 GDPR) ska varje EU-land ha en tillsynsmyndighet som övervakar de som behandlar personuppgifter. I Sverige är det Datainspektionen som är tillsynsmyndighet.

Datainspektionens uppgift är bland annat att:

- Granska att lagar och regler följs.
- Utbilda, informera och ge vägledning till de som behandlar personuppgifter.
- Följa utvecklingen inom området.
- Sprida kunskap till allmänheten och verksamheter.
- Påverka nya lagar.

Datainspektionen är även den myndighet som hanterar klagomål och överträdelser av dataförordningens regler.

2 Behandling av personuppgifter

Bromölla kommun ska se till att personuppgifter behandlas på en utpekad rättslig/laglig grund (se punkt 2.1) och att de grundläggande principerna uppfylls (se punkt 2.2). Vidare får behandling av personuppgifter ske om lämplig teknisk och organisatorisk säkerhet har säkerställts för behandlingen (se punkt 2.4).

2.1 Laglig grund för behandling av personuppgifter

Personuppgifter får endast behandlas om det finns laglig grund för behandlingen (artikel 6 GDPR). Den lagliga grunden ska fastställas innan behandling påbörjas.

En personuppgiftsbehandling är laglig om någon av nedanstående grunder kan åberopas som stöd för behandlingen:

1. Om den registrerade lämnat sitt **samtycke**[2] till behandlingen så är behandlingen tillåten.
2. Behandlingen är tillåten om den är **nödvändig för att fullgöra ett avtal** där den registrerade är part. Exempelvis att ingå ett anställningsavtal.
3. Behandlingen är tillåten om den är **nödvändig för att fullgöra en rättslig förpliktelse**, det vill säga en behandling som följs av EU-rätt eller svensk rätt. Exempel på författningar som medger rätt till personuppgiftsbehandlingar är skollagen, arkivlagen, bokföringslagen, patientregisterlagen och kameraövervakningslagen.
4. Behandlingen är tillåten om den är **nödvändig för att skydda intressen som är av grundläggande betydelse** för den registrerade eller för annan fysisk person. Denna grund handlar om sådana intressen som är av avgörande betydelse för den registrerade eller någon annans liv. Som exempel kan nämnas en personuppgiftsbehandling som är nödvändig för livsavgörande vård i akuta situationer då den registrerade inte kan lämna samtycke.
5. Behandlingen är tillåten om den är **nödvändig för att utföra en uppgift av allmänt intresse**, till exempel uppgifter som behövs för statistiska ändamål, behandling i samband med tillsynsärenden eller behandlingar som ett led i myndighetsutövning.

2.2 Grundläggande principer för behandling av personuppgifter

Vid behandling av personuppgifter ska följande gälla (artikel 5 GDPR):

- Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den enskilde (*laglighet, korrekthet och öppenhet*).

[2] Observera att myndigheter har begränsade möjligheter att använda sig av samtycke som laglig grund. Samtycke ska lämnas frivilligt och under jämlika maktförhållanden. Eftersom maktförhållandet ofta är ojämlikt i relationen mellan kommun och medborgare kan samtycke endast användas i begränsad utsträckning av kommunen.

- Personuppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål, och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (*ändamålsbegränsning*).
- Personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering*).
- Personuppgifterna ska vara korrekta och om nödvändigt uppdaterade. Åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga ska raderas eller rättas utan dröjsmål (*riktighet*).
- Personuppgifterna får inte lagras längre tid än nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifterna får lagras under längre period i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 GDPR, under förutsättning att de lämpliga tekniska och organisatoriska åtgärderna som krävs enligt dataskyddsförordningen genomförs för att säkerställa den registrerades friheter och rättigheter (*lagringsminimering*).
- Personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet, inbegripet skydd mot obehörig eller otillåten behandling samt mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (*integritet och konfidentialitet*).

2.3 Behandling av känsliga personuppgifter

Behandling av känsliga/integritetskänsliga personuppgifter är som huvudregel inte tillåten. För att behandla sådana uppgifter krävs därför att något undantag är tillämpligt (artikel 9 GDPR).

Exempel på undantag som kan vara tillämpliga i Bromölla kommuns verksamheter är:

- För att efterleva offentlighetsprincipen, till exempel i hantering av allmänna handlingar.
- För att kunna handlägga ärenden.
- I annat fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse, och inte innebär ett otillbörligt intrång i den enskildes personliga integritet.

Känsliga/integritetskänsliga personuppgifter kan kräva en högre säkerhetsnivå än mer harmlösa personuppgifter (se punkt 2.4). Om en behandling av personuppgifter ”sannolikt leder till hög risk” för den enskildes fri- och rättigheter är det ett krav att göra en konsekvensbedömning (se punkt 2.5). Känsliga/integritetskänsliga uppgifter kan vara avgörande för om en personuppgiftsincident måste anmälas till Datainspektionen (se punkt 2.6).

2.4 Personuppgifter som en del av säkerhetsarbetet

Dataskyddsförordningen ställer krav på säkerhet i samband med behandlingen (artikel 32 GDPR). Det kan handla om fysiskt skydd (exempelvis skalskydd i form av larm, lås och en säker byggnad), tekniskt skydd (exempelvis brandväggar och kryptering) eller administrativt regelverk (policys, riktlinjer och annan styrning av hur information ska hanteras av användarna).

Behandling av personuppgifter får ske om lämplig teknisk och organisatorisk säkerhet vidtagits för handlingen. Säkerheten ska baseras på genomförda informationssäkerhetsklassningar och riskanalyser. Dataskyddsombudet ska involveras.

2.5 Konsekvensbedömning

Syftet med konsekvensbedömning är att förebygga risker innan de uppkommer. Innan en konsekvensbedömning görs ska en riskanalys genomföras (se punkt 2.4).

Vid genomförande av en konsekvensbedömning avseende personuppgiftsbehandling ska dataskyddsombudet rådfrågas (artikel 35 GDPR).

En konsekvensbedömning ska enligt förordningen göras vid:

- Automatiskt beslutsfattande som grundar sig på en systematisk och omfattande bedömning av människors aspekter, till exempel profilering.
- Behandling i stor omfattning av känsliga personuppgifter eller av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott.
- Systematisk övervakning av en allmän plats i stor omfattning.

Utöver dessa situationer har Datainspektionen tagit fram en förteckning över när en konsekvensbedömning ska göras. Om två eller flera av kriterierna i förteckningen nedan är uppfyllda behöver en konsekvensbedömning sannolikt göras. Så snart en punkt är uppfylld ska en konsekvensbedömning alltid övervägas. Observera att listan inte är uttömmande. Det kan finnas andra situationer, som sannolikt innebär en hög risk, då en konsekvensbedömning ska göras.

Överväg konsekvensbedömning om personuppgiftsbehandlingen innebär att den personuppgiftsansvarige:

- Utvärderar eller poängsätter människor.
- Behandlar personuppgifter i syfte att fatta automatiska beslut som har rättsliga följder eller liknande följder för den enskilde.
- Systematiskt övervakar människor, till exempel genom kameraövervakning av en allmän plats eller genom att samla in personuppgifter från internetanvändning i offentliga miljöer.
- Behandlar känsliga personuppgifter eller uppgifter som är mycket personliga, till exempel lagring av patientjournaler.

- Behandlar personuppgifter i stor omfattning.
- Kombinerar personuppgifter från två eller flera behandlingar som ett sätt som den registrerade inte förväntar sig, till exempel när man samkör register.
- Behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning och därför är sårbara.
- Använder ny teknik eller nya organisatoriska lösningar.
- Behandlar personuppgifter på ett sätt som hindrar den enskilde från att få tillgång till en tjänst eller ingå ett avtal.

Att utföra en konsekvensbedömning är dock obligatoriskt endast om personuppgiftsbehandlingen ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”. En behandling kan uppfylla två eller flera av ovanstående kriterier men ändå bedömas att sannolikt inte leda till en hög risk för fysiska personers rättigheter och friheter. I sådana situationer bör den personuppgiftsansvarige motivera och dokumentera anledningarna till att en konsekvensbedömning inte utförs och inkludera dataskyddsombudets synpunkter.

Fyra grundläggande krav på vad en konsekvensbedömning ska innehålla:

- En systematisk beskrivning av den planerade behandlingen och behandlingens syfte.
- En bedömning av om behandlingen är nödvändig och proportionerlig i förhållande till syftet med den.
- En bedömning av riskerna för de registrerades rättigheter och friheter.
- De åtgärder som planeras för att hantera riskerna och för att visa att dataskyddsförordningen efterlevs.

Dessutom måste:

- Dataskyddsombudet rådfrågas.
- Synpunkter inhämtas från den enskilde eller dess företrädare när det är lämpligt.

I konsekvensbedömningen ska det tydligt dokumenteras vad som ska göras för att garantera säkerheten i personuppgiftsbehandlingen.

Om risken med en personuppgiftsbehandling bedöms hög, och fortsatt bedöms hög även efter att planerade åtgärder för att minska riskerna vidtagits, ska förhandssamråd med Datainspektionen ske.

Vid begäran om förhandssamråd ska Datainspektionen kontaktas, se information på deras hemsida.

Innan förhandssamråd begärs ska riskanalys och konsekvensbedömning genomförts och dokumenterats. Dokumentationen ska innehålla en redogörelse för vilka risker som kvarstår och varför de inte kunnat åtgärdas.

2.6 Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risk för en eller flera personers rättigheter och friheter.

Exempel på personuppgiftsincidenter är när uppgifter om en eller flera personer har:

- Blivit förstörda.
- Gått förlorade på annat sätt.
- Kommit i orätta händer.

Riskerna det medför kan till exempel vara:

- Diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning.
- Finansiell förlust.
- Brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident ska anmälas till Datainspektionen inom 72 timmar efter att incidenten upptäckts. Datainspektionens digitala e-tjänst (som nås på deras hemsida) ska användas.

En incident behöver inte anmälas om det är osannolikt att den innebär en risk för den enskildes rättigheter och friheter. Det räcker då att motivera beslutet att inte anmäla och noga dokumentera incidenten. Dokumentationen ska omfatta omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Om en personuppgiftsincident leder till en hög risk för den enskilde, ska den enskilde informeras om incidenten. Hög risk kan vara att personuppgiftsincidenten är allvarlig och/eller att sannolikheten för konsekvenser är stor.

2.7 Informationsskyldighet

Information om hur personuppgifter behandlas ska lämnas av personuppgiftsansvarig både när uppgifterna samlas in och när den enskilde annars begär det (artiklarna 13-14 GDPR).

Om personuppgifterna samlas in *från den enskilde själv* behöver den enskilde inte informeras om denne redan har informationen.

Om personuppgifterna samlas in *på något annat sätt än från den enskilde* behöver den enskilde inte informeras om:

- Den enskilde redan har fått informationen.
- Det är omöjligt eller skulle innebära en oproportionerligt stor ansträngning att informera.
- Om registreringen eller utlämnandet av uppgifterna föreskrivs genom lag.
- Personuppgifterna omfattas av sekretess enligt lag.

Vidare ska berörd individ informeras om en eventuell personuppgiftsincident inträffat, om personuppgiftsincidenten bedöms kunna leda till en hög risk för den enskilde (se punkt 2.6).

2.8 Register över behandling (registerförteckning)

Både personuppgiftsansvariga (se punkt 1.5) och personuppgiftsbiträden (se punkt 1.6) är skyldiga att föra ett register eller en förteckning över behandlingar av personuppgifter. Dessa register ska upprättas skriftligen, vara tillgängliga i elektroniskt format och hållas uppdaterad. På begäran ska registret göras tillgängligt för Datainspektionen. Vad som ska finnas med i registret/förteckningen beskrivs i artikel 30, GDPR.

Checklista på vad registret ska innehålla för personuppgiftsansvariga:

- Namn och kontaktuppgifter för den personuppgiftsansvarige, den personuppgiftsansvariges företrädare samt dataskyddsombudet.
- Ändamålen med behandlingen.
- En beskrivning av kategorierna av registrerade och kategorierna av personuppgifter.
- De kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.
- I tillämpliga fall, överföringar av personuppgifter till ett tredjeland eller en internationell organisation.
- Om möjligt, de förutsedda tidsfristerna för radering av de olika kategorierna av uppgifter.
- Om möjligt, en allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder.

2.9 Bevarande och gallring

En grundläggande princip i dataskyddsförordningen är att personuppgifter inte ska sparas längre än nödvändigt (se punkt 2.2). Arkivlagen, där bevarande och gallring involveras, har företräde framför dataskyddsförordningen.

En informationshanteringsplan, även kallad dokumenthanteringsplan, tar upp vad som gäller.

2.10 Checklista innan behandling av personuppgifter påbörjas

Innan behandling av personuppgifter påbörjas krävs följande:

1. Identifiera och dokumentera vilka personuppgifter som kommer att behandlas.
2. Dokumentera ändamål och syfte med behandlingen samt hur länge behandlingen kommer att pågå.
3. Fastställ laglig grund (se punkt 2.1).
4. Inhämta samtycke vid behov.

5. Säkerställ att det finns rättslig grund att behandla känsliga/integritetskänsliga personuppgifter om detta är aktuellt (se punkt 1.3 och 2.3).
6. Säkerställ att behandlingen sker i enlighet med de grundläggande principerna (se punkt 2.2) och policyn för hantering av personuppgifter samt dessa riktlinjer.
7. Vid behov, rådgör med dataskyddsombudet (se punkt 1.9).
8. Klassificera personuppgifterna utifrån informationssäkerhetsnivå och genomförd riskanalys (se punkt 2.4). Vid behov ska en konsekvensbedömning göras (se punkt 2.5).
9. Samråd med Datainspektionen om eventuell konsekvensbedömning visar att det finns en hög risk med behandlingen som inte kan åtgärdas (se punkt 2.5).
10. Se till att det finns tillräckliga tekniska och organisatoriska säkerhetsåtgärder utifrån genomförd informationssäkerhetsklassning och resultat från genomförd riskanalys (se punkt 2.4).
11. Informera den enskilde om behandlingen om det finns ett sådant krav (se punkt 2.7).
12. Upprätta personuppgiftsbiträdeavtal vid behov (se punkt 1.7).
13. Anteckna ny behandling i registerförteckningen (se punkt 2.8).

3 Om dataskyddsförordningen inte följs

Datainspektionen kan utfärda varningar om en planerad behandling sannolikt kommer att bryta mot bestämmelserna i dataskyddsförordningen, och utfärda reprimander om en pågående behandling av personuppgifter bryter mot bestämmelserna.

Datainspektionen kan besluta att ett företag som bryter mot reglerna i dataskyddsförordningen ska betala en administrativ sanktionsavgift. Avgiften kan som mest vara 20 miljoner euro eller fyra procent av bolagets globala årsomsättning, beroende på vilket belopp som är högst. För de något mindre allvarliga överträdelserna gäller ett maxbelopp på 10 miljoner euro eller 2 procent av den globala årsomsättningen. Svenska myndigheter kan maximalt få 10 miljoner kronor i sanktionsavgift.

Enligt artikel 82 GDPR ska varje person som lidit materiell eller immateriell skada till följd av en överträdelse av dataskyddsförordningen ha rätt till ersättning från den personuppgiftsansvarige, eller personuppgiftsbiträdet, för den uppkomna skadan.