Innehåll

1 Allmänna bestämmelser 3
1.1 Inledning 3
1.2 Syfte 3
1.3 Materiellt tillämpningsområde 3
1.4 Territoriellt tillämpningsområde 3
1.5 Lagstiftning 4
1.6 Ändring av policy 4
1.7 Definitioner 4
personuppgifter 4
känsliga personuppgifter 4
behandling 4
register 4
samtycke av den registrerade 5
personuppgiftsansvarig 5
personuppgiftsbiträde 5
dataskyddsombud 5
begränsning av behandling 5
personuppgiftsincident 5
2 Principer 6
2.1 Principer för behandling av personuppgifter 6
Laglighet, korrekthet och öppenhet 6
Ändamålsbegränsning 6
Uppgiftsminimering 6
korrekthet 6
lagringsminimering 6
integritet och konfidentialitet 6
ansvarsskyldighet 7
2.2 Villkor för samtycke 7
2.3 Behandling av särskilda kategorier av personuppgifter 7
3 Den registrerades rättigheter 7
3.1 Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter 7
3.2 Det ska framgå om personuppgifterna har samlats in från den registrerade eller kommer från annan part. 8

3.3 Den registrerades rätt till tillgång ... 8
3.4 Rätt till rättelse ... 8
3.5 Rätt till radering (”rätten att bli bortglömd”) ... 8
3.6 Rätt till begränsning av behandling ... 8
3.7 Rätt till dataportabilitet ... 9
3.8 Rätt att göra invändningar ... 9
4 Personuppgiftsansvarig och personuppgiftsbiträde ... 9
4.1 Säkerhet i samband med behandlingen ... 9
4.2 Gemensamt personuppgiftsansvariga ... 9
4.3 Personuppgiftsbiträden ... 10
4.4 Samarbete med tillsynsmyndigheten ... 10
4.5 Personuppgiftsincident ... 10
4.6 Konsekvensbedömning avseende dataskydd ... 11
4.7 Utnämning av dataskyddsombud ... 11
4.8 Dataskyddsombudets ställning ... 11
4.9 Dataskyddsombudets uppgifter ... 12
5 Överföring av personuppgifter ... 12
6 Rättsmedel, ansvar och sanktioner ... 13
7 Behandling i anställningsförhållanden ... 13
8 Slutbestämmelser ... 13
9 Ledningens och styrelsens godkännande ... 13

1 Allmänna bestämmelser

Denna policy gäller för både Apotek Produktion & Laboratorier AB och det helägda dotterbolaget APL Fastigheter AB som äger de lokaler där APL bedriver verksamhet. Nedan benämns dessa två bolag endast som APL.

1.1 Inledning

APL har ett viktigt samhällsuppdrag – att utveckla och tillhandahålla individanpassade läkemedel till patienter med särskilda behov. För att säkerställa att alla patienter får tillgång till rätt behandling sker vårt arbete i nära dialog med specialister, apotek, landsting och myndigheter. Vid sidan av vårt samhällsuppdrag utvecklar och kontraktstillverkar vi läkemedel och medicintekniska produkter på uppdrag av bioteknik-, medicinteknik- och läkemedelsföretag. Vi tillverkar också egna medicintekniska produkter.

Det är av yttersta vikt för APL att skydda våra kunders, patienters, leverantörers, affärspartners och medarbetares personuppgifter. Brott mot dataskyddslagstiftningen kan få allvarliga konsekvenser och böter. Den allvarligaste konsekvensen är om patient- och integritetsskyddet bryts samt om vårt anseende skadas. I denna policy beskrivs de åtgärder som APL ska vidta i syfte att skydda integriteten och konfidentialiteten för de personuppgifter som behandlas inom vår verksamhet.

1.2 Syfte

I denna policy beskrivs de bestämmelser som gäller vid behandling av personuppgifter för APL i syfte att skydda de registrerade. Syftet med denna policy är att skydda den registrerades grundläggande fri- och rättigheter i enlighet med dataskyddslagstiftningen (inklusive, men inte begränsat till, den europeiska allmänna dataskyddsförordningen (GDPR)).

1.3 Materiellt tillämpningsområde[1]

Denna policy avser personuppgifter som kan identifiera fysiska personer och som systematiskt lagras elektroniskt eller i pappersform, som inte lyder under lagstiftning (rättslig förpliktelse) överordnad Dataskyddsförordningen (GDPR). Denna policy är avsedd att användas tillsammans med APLs befintliga policyer.

APLs verksamhet lyder även under andra regelverk så som GMP (Good Manufacturing Practice) som i sig är överordnad GDPR.

1.4 Territoriellt tillämpningsområde[2]

Denna policy ska tillämpas inom APLs samtliga verksamheter.

[1] Art. 2 i dataskyddsförordningen.
[2] Art. 3 i dataskyddsförordningen.

1.5 Lagstiftning

Denna policy bygger på bestämmelserna i den europeiska dataskyddslagstiftningen (särskilt dataskyddsförordningen EU 2016/679 (GDPR) som fastställer höga dataskyddskrav och gäller i alla EU:s medlemsstater.

1.6 Ändring av policy

APLs ledning förbehåller sig rätten att ändra eller modifiera denna policy i samråd med ansvarigt dataskyddsombud. De anställda på APL måste följa bestämmelserna i denna policy.

1.7 Definitioner[3]

Nedan följer en sammanfattning av definitioner (i enlighet med dataskyddsförordningen på begrepp som används i denna policy.

personuppgifter

Personuppgifter är uppgifter som direkt eller indirekt kan kopplas till en person. Det kan vara självklara uppgifter som namn eller personnummer, men även uppgifter som till exempel e-postadress eller signatur. Även bilder är en form av personuppgift, om en person tydligt kan urskiljas på bilden.

känsliga personuppgifter

Personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning,

I dataskyddsförordningen kallas de här uppgifterna särskilda kategorier av personuppgifter.

behandling

En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, 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,

register

En strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

[3] Art. 4 i dataskyddsförordningen.

samtycke av den registrerade

När den registrerade frivilligt har sagt ja till personuppgiftsbehandlingen.

personuppgiftsansvarig

En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som bestämmer för vilka ändamål personuppgifterna ska behandlas och hur behandlingen ska gå till.

personuppgiftsbiträde

En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

dataskyddsombud

företagets dataskyddsombud (DPO) har till uppgift att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser.

begränsning av behandling

Markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden.

personuppgiftsincident

När de personuppgifter vi behandlar olagligt förstörs, förvanskas, försvinner eller ändras. När någon som inte har behörig tillgång till personuppgifterna får tillgång/åtkomst till dessa. När personuppgifterna på ett obehörigt sätt röjs (obehörigt röjande).

särskilda kategorier av personuppgifter

Se känsliga personuppgifter

2 Principer

2.1 Principer för behandling av personuppgifter[4]

Laglighet, korrekthet och öppenhet[5]

Behandlingen ska ske på ett lagligt, korrekt och öppet sätt. Behandlingen är endast laglig om åtminstone ett av följande villkor är uppfyllt:

a) den registrerade har lämnat sitt samtycke (se avsnitt 2.2 i denna policy)
b) behandlingen är nödvändig för att fullgöra ett avtal
c) behandlingen är nödvändig för att fullgöra en rättslig förpliktelse eller
d) behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen.

Ändamålsbegränsning[6]

Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Kontakta dataskyddsombudet i förväg (innan planer införs) om ändamålen med behandlingen ändras.

Uppgiftsminimering

Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Uppgifterna ska raderas om de inte längre behövs. APLs ledning ska säkerställa att kraven avseende lagring och radering uppfylls. Alla medarbetare ska granska sina register regelbundet och om lämpligt radera dem för att uppfylla kraven. Den som ansvarar för respektive register ser till att dessa granskningar utförs.

Alla medarbetare har en skyldighet att påtala brister i registerhanteringen.

Mer information finns i Riktlinjer för lagring av register.

korrekthet

Personuppgifter ska vara korrekta och om nödvändigt uppdaterade i förhållande till de ändamål för vilka de behandlas.

lagringsminimering[7]

Personuppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

integritet och konfidentialitet[8]

Personuppgifter ska behandlas på ett säkert sätt. De ska genom tekniska eller organisatoriska åtgärder skyddas mot obehörig eller otillåten behandling, förlust, förstöring eller skada.

[4] Art. 5 i dataskyddsförordningen.
[5] Art. 6 i dataskyddsförordningen.
[6] Art. 5 i dataskyddsförordningen.
[7] Art. 5 i dataskyddsförordningen.
[8] Art. 5 i dataskyddsförordningen.

ansvarsskyldighet

APL ska, som personuppgiftsansvarig, ansvara för och kunna visa att principerna från dataskyddsförordningen som anges ovan efterlevs. Alla medarbetare ska genomgå APLs dataskyddsutbildning.

APL ska föra ett fullständigt register över behandlingsåtgärder[9]. Den som ansvarar för ett enskilt register måste informera APLs dataskyddsombud (DPO) i god tid innan ny eller ändrad behandling av personuppgifter införs, så att registren kan anpassas.

2.2 Villkor för samtycke[10]

Om den registrerade frivilligt godkänt behandling av personuppgifter som rör honom eller henne, måste dessutom följande villkor vara uppfyllda:

a) Samtycket ska lagras så att man kan visa på att samtycke skett.
b) När APL ber om skriftligt samtycke ska det särskiljas från andra eventuella frågor.
c) Den registrerade ska ha rätt att när som helst enkelt återkalla sitt samtycke. Innan samtycke lämnas ska den registrerade informeras om hur samtycket kan återkallas.

Kontakta APLs dataskyddsombud för mallar för samtyckesformulär.

2.3 Behandling av särskilda kategorier av personuppgifter[11]

Behandling av särskilda personuppgifter är förbjuden, såvida inte

a) den registrerade har lämnat sitt samtycke
b) behandlingen är nödvändig inom områden som arbetsrätten och social trygghet
~~c)~~ behandlingen är nödvändig för skäl som hör samman med medicinska diagnoser, tillhandahållande av hälso- och sjukvård, social omsorg eller behandling

3 Den registrerades rättigheter

3.1 Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter

Samtliga registrerade har följande rättigheter:

- Rätt till tillgång
- Rätt till rättelse
- Rätt till radering
- Rätt till begränsning av behandling
- Rätt till dataportabilitet
- Rätt att göra invändningar

[9] Art. 30 i dataskyddsförordningen.
[10] Art. 7 i dataskyddsförordningen.
[11] Art. 9 i dataskyddsförordningen.

APL ska, som personuppgiftsansvarig, kontrollera identiteten på den registrerade innan någon åtgärd enligt ovan vidtas.

All information och kommunikation som avser behandling som lämnas till den registrerade ska vara tydlig. Informationen ska ges skriftligt utan dröjsmål, dock senast inom en månad.

3.2 Det ska framgå om personuppgifterna har samlats in från den registrerade eller kommer från annan part.[12]

Oavsett om personuppgifterna kommer direkt från den registrerade eller inte är APL skyldig att lämna den informationen till den registrerade. Detta ska ske antingen vid insamling eller inom en rimlig period efter det att uppgifterna har erhållits från annan källa. Detta måste dock göras inom en månad. Kontakta APLs dataskyddsombud för exempel på informationsmallar.

3.3 Den registrerades rätt till tillgång[13]

Den registrerade ska ha rätt att av APL, som personuppgiftsansvarig, få bekräftelse på om personuppgifter som rör honom eller henne behandlas i verksamheten. Den registrerade kan då begära att få tillgång till personuppgifterna och ändamålen med behandlingen. Kontakta APLs dataskyddsombud för att kontrollera om och hur en sådan begäran om tillgång ska besvaras.

3.4 Rätt till rättelse[14]

Den registrerade har rätt att få felaktiga personuppgifter som rör honom eller henne rättade och att få ofullständiga personuppgifter kompletterade. En sådan begäran ska behandlas utan onödigt dröjsmål.

3.5 Rätt till radering (”rätten att bli bortglömd”)[15]

Den registrerade har rätt att begära att få sina personuppgifter raderade, t.ex. om personuppgifterna inte längre är nödvändiga för de ändamål som APL ursprungligen samlade in dem, eller om den registrerade återkallar sitt samtycke.

3.6 Rätt till begränsning av behandling[16]

Den registrerade har rätt att kräva att få behandlingen av sina personuppgifter begränsade, t.ex. om APL, som personuppgiftsansvarig, inte längre behöver personuppgifterna, men den registrerade behöver dem för rättsliga anspråk. Kontakta APLs dataskyddsombud i dessa fall.

[12] Art. 13 och 14 i dataskyddsförordningen
[13] Art. 15 i dataskyddsförordningen.
[14] Art. 16 i dataskyddsförordningen.
[15] Art. 17 i dataskyddsförordningen.
[16] Art. 18 i dataskyddsförordningen.

3.7 Rätt till dataportabilitet[17]

Den registrerade har rätt att få kopior på de personuppgifter som han eller hon har tillhandahållit APL, som personuppgiftsansvarig, i ett strukturerat, allmänt använt och maskinläsbart format. Den registrerade har rätt att begära att personuppgifterna överförs från den personuppgiftsansvarige till en annan personuppgiftsansvarig. Detta gäller när behandlingen grundar sig på samtycke eller på ett avtal och behandlingen sker automatiserat. Kontakta APLs dataskyddsombud i dessa fall.

3.8 Rätt att göra invändningar[18]

Den registrerade har rätt att när som helst göra invändningar mot behandling av personuppgifter rörande honom eller henne, i synnerhet vid behandling för direkt marknadsföring, profilering och forskningsändamål. APL får, som personuppgiftsansvarig, inte längre behandla personuppgifterna om det inte finns tvingande berättigade skäl för behandlingen. Kontakta APLs dataskyddsombud i dessa fall.

4 Personuppgiftsansvarig och personuppgiftsbiträde

4.1 Säkerhet i samband med behandlingen

APL ska, som personuppgiftsansvarig, vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken[19]. Detta för att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna, som beskrivs i APLs IT-säkerhetspolicy. Den personuppgiftsansvarige ska också säkerställa inbyggt dataskydd och dataskydd som standard, så att nödvändiga skyddsåtgärder för att genomföra dataskyddsprinciper (se 2.1) integreras. Detta kommer att bidra till att säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas.[20] För att säkerställa att ledningssystemet för informationssäkerhet ständigt förbättras och för att garantera anpassning till nya tekniska krav har periodiska översyner och revisionsprocesser införts.[21] Affärskontinuitet och katastrofplanering införs för att säkerställa förmågan att återställa tillgängligheten och tillgången till personuppgifter inom rimlig tid vid en fysisk eller teknisk incident.

4.2 Gemensamt personuppgiftsansvariga

Om två eller flera personuppgiftsansvariga (t.ex. APL tillsammans med en extern tjänsteleverantör) gemensamt fastställer ändamålen med och medlen för behandlingen av personuppgifter ska de vara gemensamt personuppgiftsansvariga och behöver ett skriftligt avtal. Kontakta APLs dataskyddsombud för mer information.[22]

[17] Art. 20 i dataskyddsförordningen.
[18] Art. 21 i dataskyddsförordningen.
[19] Art. 24 i dataskyddsförordningen.
[20] Art. 25 i dataskyddsförordningen.
[21] Art. 32 i dataskyddsförordningen.
[22] Art. 26 i dataskyddsförordningen.

4.3 Personuppgiftsbiträden[23]

Behandling som genomförs för personuppgiftsansvarigs räkning (t.ex. av en tjänsteleverantör inom IT eller HR) är endast tillåten om personuppgiftsbiträdet ger tillräckliga garantier om att säkerställa att den registrerades rättigheter skyddas och om ett avtal har slutits. Personuppgiftsbiträdet ska väljas ut noga och regelbundet granskas. Be APLs dataskyddsombud om ett avtal och en revisions-mall.

Detsamma gäller om APL behandlar personuppgifter för en annan organisations räkning (t. ex. kund)

Dessutom måste åtgärder vidtas för att säkerställa att personuppgiftsbiträdet följer de informationssäkerhetsstandarder som anges i APLs IT-säkerhetspolicy och endast behandlar personuppgifter enligt instruktionerna.[24] Det är förbjudet att behandla personuppgifter tillhörande en EU-medborgare om behandlingen sker utanför EU, såvida inte de särskilda villkoren avseendeöverföring av personuppgifter är uppfyllda (se kapitel 5 i denna policy).

4.4 Samarbete med tillsynsmyndigheten

APL och dess medarbetare är skyldiga att samarbeta med Datainspektionen. Om du som anställd kontaktas av Datainspektionen ska du enbart bekräfta mottagande av meddelande och sedan omedelbart kontakta APLs dataskyddsombud.25

4.5 Personuppgiftsincident

Alla personuppgiftsincidenter ska omedelbart rapporteras till APLs dataskyddsombud av medarbetaren eller avdelningschefen. Om incidenten sannolikt leder till en hög risk för de registrerades fri- och rättigheter ska den registrerade informeras om detta utan onödigt dröjsmål.[26] Om personuppgiftsincidenten sannolikt leder till en risk för de registrerades fri- och rättigheter ska den lokala tillsynsmyndigheten utan onödigt dröjsmål informeras (av APL dataskyddsombud). Detta måste göras inom 72 timmar efter att man har fått vetskap om incidenten.[27]

För att minska de risker som en personuppgiftsincident medför och för att underlätta rapporteringen till både tillsynsmyndigheterna och de berörda registrerade måste motsvarande process för personuppgiftsincidenter följas vid respektive personuppgiftsincident, i syfte att säkerställa att kraven i dataskyddslagstiftningen uppfylls. Mer information finns i ”Riktlinjer för personuppgiftsincidenter”.

Vid frågor om dataskydd eller om du misstänker att personuppgifter behandlas felaktigt kan du kontakta APLs dataskyddsombud.

[23] Art. 28 i dataskyddsförordningen.
[24] Art. 29 i dataskyddsförordningen.
[25] Art. 31 i dataskyddsförordningen.
[26] Art. 34 i dataskyddsförordningen.
[27] Art. 33 i dataskyddsförordningen.

4.6 Konsekvensbedömning avseende dataskydd

En konsekvensbedömning avseende dataskydd[28] krävs före behandling om behandlingen av uppgifter, i synnerhet när ny teknik används, sannolikt leder till en hög risk för de registrerades fri- och rättigheter.

En konsekvensbedömning avseende dataskydd krävs vid:

1) Användning av ny teknik.
2) Automatisk behandling på vilken beslut grundar sig som har rättsliga följder för fysiska personer.
3) Behandling i stor omfattning av särskilda kategorier av personuppgifter (ursprung, politiska åsikter, religion eller sexuell läggning).
4) Behandling av uppgifter rörande brott och brottmål.
5) Systematisk övervakning av en allmän plats i stor omfattning.

För att säkerställa att konsekvensbedömningen slutförs innan ny eller ändrad behandling av personuppgifter påbörjas, måste medarbetaren informera APLs dataskyddsombud i förväg (innan planerna införs). Kontakta APLs dataskyddsombud som kan tillhandahålla mallar för konsekvensbedömning avseende dataskydd, vägledning och löpande rådgivning.

Dataskyddsombudet ska samråda med Datainspektionen om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk för de registrerades fri- och rättigheter om inte den personuppgiftsansvarige vidtar åtgärder för att minska riskerna.

4.7 Utnämning av dataskyddsombud[29]

APL har utnämnt ett dataskyddsombud. Dataskyddsförordningen anger att ett dataskyddsombud bör utnämnas om kärnverksamheten består av behandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning eller om kärnverksamheten består av behandling i stor omfattning av särskilda kategorier av uppgifter.

Dataskyddsombudets uppgift är att övervaka om APLs policyer (denna policy samt detaljerade policyer) följs, i syfte att utveckla och uppdatera dem.

Rollen som utses ska ha erforderliga yrkesmässiga kvalifikationer och kunskaper om lagstiftning och praxis avseende dataskydd.

4.8 Dataskyddsombudets ställning[30]

Dataskyddsombudet ska på ett korrekt sätt och i god tid delta i alla frågor, projekt, förändringar eller åtgärder som rör bestämmelserna om skyddet av personuppgifter.

APL, i egenskap av personuppgiftsansvarig ska stödja dataskyddsombudet i utförandet av arbetsuppgifter genom att tillhandahålla de resurser som krävs samt ge tillgång till personuppgifter och behandlingsförfaranden. Dataskyddsombudets sakkunskap ska upprätthållas.

[28] Art. 35 i dataskyddsförordningen.
[29] Art. 38 i dataskyddsförordningen.
[30] Art. 38 i dataskyddsförordningen.

Dataskyddsombudet ska ha en oberoende och skyddad ställning inom organisationen och ska rapportera till högsta förvaltningsnivå.

Dataskyddsombudet ska fungera som naturlig kontaktpunkt för alla registrerade i frågor som rör behandlingen av deras personuppgifter samt vara kontaktpunkt för tillsynsmyndigheten.

Dataskyddsombudet ska vara bunden av sekretess och/eller konfidentialitet när det gäller genomförandet av deras uppgifter.

Kontaktuppgifter till ansvarigt dataskyddsombud ska publiceras på APLs intranät, APPELL samt externwebb, www.apl.se.

4.9 Dataskyddsombudets uppgifter[31]

Dataskyddsombudet ska ansvara för att informera och ge råd till APL i egenskap av personuppgiftsansvarig eller personuppgiftsbiträde, samt till APLs medarbetare.

APLs ledning ska, som personuppgiftsansvarig, säkerställa att bestämmelserna om dataskydd som beskrivs i lagar, förordningar och koncernövergripande policyer följs. Ledningen ansvarar särskilt för att skydda de registrerades rättigheter.

Dataskyddsombudet ska ansvara för att övervaka efterlevnaden av dataskyddsförordningen, lokala lagar och förordningar avseende dataskydd, denna policy och andra angivna APL-policyer för att skydda de registrerades grundläggande fri- och rättigheter i samband med behandling av personuppgifter.

5 Överföring av personuppgifter

Överföring av personuppgifter inom det land där uppgifterna har samlats in, inom Europeiska unionen (EU) och Europeiska ekonomiska samarbetsområdet (EES) (inklusive behandling i ett tredjeland efter överföring) är i allmänhet tillåtet om behandlingen av uppgifterna också är tillåten enligt dataskyddsförordningen (särskilt i enlighet med kapitel II).

Personuppgifter får endast överföras från ett EU-/EES-land till ett tredjeland (utanför EU/EES) om särskilda villkor är uppfyllda. Kontakta ansvarigt dataskyddsombud i dessa fall. Överföring får ske:

- om Europeiska kommissionen har beslutat att tredjelandet säkerställer en adekvat skyddsnivå (”beslut om adekvat skyddsnivå”, t.ex. Schweiz)[32]
- om den mottagande parten har vidtagit lämpliga skyddsåtgärder (t.ex. bindande företagsbestämmelser, standardiserade dataskyddsbestämmelser som antagits av kommissionen, en godkänd uppförandekod)[33]
- vid domstolsbeslut eller beslut från myndigheter om det grundar sig på en internationell överenskommelse[34]
- om överföringen sker i särskilda situationer (t.ex. uttryckligt samtycke från den registrerade, om överföringen är nödvändig för att fullgöra ett avtal, om överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk,

[31] Art. 39 i dataskyddsförordningen.

[32] Art. 45 i dataskyddsförordningen.

[33] Art. 46 i dataskyddsförordningen.

[34] Art. 48 i dataskyddsförordningen.

om överföringen är nödvändig för att skydda den registrerades grundläggande intressen)[35]
- om överföringen är nödvändig för ändamål som rör den personuppgiftsansvariges tvingande berättigade intressen och den personuppgiftsansvarige informerar tillsynsmyndigheten[36].

6 Rättsmedel, ansvar och sanktioner

Följande rättsmedel är tillgängliga:

- Den registrerades rätt att lämna in klagomål till en tillsynsmyndighet[37].
- En fysisk eller juridisk persons rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut[38].
- Den registrerades rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde[39].
- Den registrerades rätt att anlita ett organ, en organisation eller en sammanslutning utan vinstsyfte[40].

Överträdelser av bestämmelserna kring dataskydd kan leda till att den registrerade lämnar in skadeståndsanspråk avseende ersättning för materiella eller immateriella skador[41]. Myndigheterna kan påföra administrativa sanktionsavgifter på upp till 10 eller 20 miljoner euro, eller, om det gäller ett företag, på upp till 2 eller 4 % av APLs totala årsomsättning under föregående budgetår[42]. Enligt svensk lag kan överträdelser leda till åtal[43]. Överträdelser från enskilda medarbetares sida kan leda till påföljder enligt svenska disciplinära åtgärder som är förenliga med svensk arbetsrätt.

7 Behandling i anställningsförhållanden

Enligt svensk lag kan det finnas mer specifika regler i lag eller i kollektivavtal för behandling av anställdas personuppgifter i anställningsförhållanden[44].

8 Slutbestämmelser

Denna policy ska tillämpas från och med den 25 maj 2018.

9 Ledningens och styrelsens godkännande

Denna dataskyddspolicy godkändes av företagsledningen den 2019-03-08 och av APLs styrelse den 2019-04-01.

---

[35] Art. 49 i dataskyddsförordningen.
[36] Art. 49, punkt 1 i dataskyddsförordningen, i slutet.
[37] Art. 77 i dataskyddsförordningen.
[38] Art. 78 i dataskyddsförordningen.
[39] Art. 79 i dataskyddsförordningen.
[40] Art. 80 i dataskyddsförordningen.
[41] Art. 82 i dataskyddsförordningen.
[42] Art. 83 i dataskyddsförordningen.
[43] Art. 84 i dataskyddsförordningen.
[44] Art. 88 i dataskyddsförordningen.