Policy GDPR för Innovatum AB, Innovatum Science Center AB, Innovatum Portfolio AB samt Innovatum Progress AB

- Bakgrund, punkt 1.
- Personuppgiftspolicy, punkt 2.

Stödjande dokument

- Bilaga 1: förslagstexter vid insamling/samtycke för Startup, ACT, Projektarena, anställda, styrelseledamöter samt Innovatum Science Center.
- Anhöriglista GDPR mall

1. Bakgrund

Dataskyddsförordningen

Europaparlamentets och rådets förordning (EU) 2016/679 beslutade den 27 april 2016 om skydd för **fysiska personer** med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

Rätten till skydd av personuppgifter kommer i grunden genom den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Utifrån dessa har Europeiska Unionens Stadga om de grundläggande rättigheterna 2016/C 202/02 utarbetats, vars 8:e artikel Dataskyddsförordningen bygger på.

Dataskyddsförordningen kallas ofta GDPR efter den engelska benämningen, ”General Data Protection Regulation”.

Artikel 8 Europeiska Unionens Stadga om de grundläggande rättigheterna

1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.
2. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.
3. En oberoende myndighet ska kontrollera att dessa regler efterlevs.

Dataskyddsförordningen gäller som lag i alla EU:s medlemsländer från och med den 25 maj 2018. Förordningen innehåller 99 artiklar.

Dataskyddsförordningens syfte

Att skydda personuppgifter. Gäller endast fysiska personer.

Tillsynsmyndighet

I Sverige är det Datainspektionen som är oberoende tillsynsmyndighet för behandling av personuppgifter.

Grundläggande principer

- Laglighet, korrekthet, öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering

- Korrekthet
- Lagringsminimering
- Integritet och konfidentialitet

Registrerade rättigheter

- Rätt att kostnadsfritt få ut information om vilka uppgifter som behandlas (registerutdrag)
- Rätt att få sina personuppgifter rättade eller raderade (”rätten att bli bortglömd”)
- Rätt att kräva att personuppgifter flyttas (portabilitet)
- Rätt att invända mot att personuppgifterna används för direktmarknadsföring
- Rätt at invända mot behandling som baseras på intresseavvägning
- Rätt att invända mot att personuppgifterna används för automatiserat beslutsfattande och profilering
- Rätt att klaga till Datainspektionen

Rättsliga grunder

Behandling är endast lag om och i den mån den baseras på någon av dessa rättsliga grunder:

Samtycke
Avtal
Rättslig förpliktelse
Grundläggande intresse för den registrerade eller annan
Allmänt intresse/myndighetsutövning
Intresseavvägning

Samtycke

Den registrerade samtycker till att dennes personuppgifter behandlas för ett eller flera specifika ändamål

- samtycke måste lämnas frivilligt - inte frivilligt om genuin valmöjlighet saknas (jfr anställning)
- lämnas skriftligt (även elektroniskt) eller muntligt
- begäran om samtycke skall vara tydligt och kortfattat
- inte tyst samtycke, t.ex. på förhand ikryssad ruta på webbplats
- skall gälla behandling av ett preciserat ändamål
- den registrerade kan när som helst återkalla sitt samtycke

Avtal

Behandlingen nödvändig för att fullgöra avtal eller för att vidta åtgärder på begäran av den registrerade innan avtal ingås

- gäller bara avtal i vilka den registrerade är eller avser att bli part, t.ex. kund- och personaladministrativa system för bl.a. fakturering respektive löneberäkning

Rättslig förpliktelse

Behandlingen nödvändig för att fullgöra rättslig förpliktelse

- gäller EU-bestämmelse, svensk lag, förelägganden, myndighetsbeslut, domar, kollektivavtal

- rättsliga förpliktelsen skall åligga PUA, t.ex. bokföringsskyldighet enligt Bokföringslagen

Grundläggande intressen

Behandlingen nödvändig för att skydda intressen av grundläggande betydelse för den registrerade eller annan fysisk person

- avgörande betydelse för den registrerades eller någon annan persons liv, t.ex. personuppgiftsbehandling som är nödvändig för livsavgörande vård i akuta situationer (den registrerade inte kan lämna samtycke) eller vid naturkatastrofer.

Allmänt intresse/myndighetsutövning

Behandlingen nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i PUAs myndighetsutövning

- allmänt intresse t.ex. skatteverkets verksamhet, arkivering, forskning och statistik, privat skola, hälso- och sjukvård, järnvägstransporter, elektronisk kommunikation, postbefordran och elproduktion
- privat myndighetsutövning, t.ex. bilbesiktning, vinstsyfte saknar betydelse
- inte offentlig verksamhet som inte innebär tvång mot enskild (t.ex. rådgivning eller undervisning)

Intresseavvägning

Behandlingen nödvändig för PUAs eller tredje mans berättigade intressen - om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre

- barn särskilt skyddsvärda
- myndigheter kan inte åberopa intresseavvägning
- om registrerad invänder måste ny intresseavvägning göras och behandlingen upphöra om inte tvingande berättigade skäl finns, t.ex. direktmarknadsföring, inom koncerner för interna administrativa ändamål, skydda elektroniska kommunikationssystem.

Register över behandling

PUA och PUB skall föra register över sina behandlingar av personuppgifter, bl.a.

- ändamålen med behandlingen
- kategorier av registrerade
- kategorier av personuppgifter
- externa mottagare av personuppgifterna
- om uppgifter förs över till tredjeland

På begäran skall PUA/PUB göra registret tillgängligt för DI

2. Personuppgiftspolicy för Innovatum

Bakgrund

Syftet med Personuppgiftspolicyn är att **fysisk person** vars personuppgifter registrerats ska få veta hur Innovatum behandlar personuppgifterna, vad de används till, vilka som får ta del av dem samt hur personen kan ta tillvara sina rättigheter.
Innovatum är Personuppgiftsansvarig (PUA) för de personuppgifter som förekommer i verksamheten och är den som bestämmer ändamålen med och medlen för behandling av de personuppgifter som förekommer inom organisationen.

Definitioner

I denna Personuppgiftspolicy används följande definitioner som har den betydelse som framgår av gällande personuppgiftslagstiftning: ”behandling, ”personuppgifter”, ”Personuppgiftsansvarig”, ”Personuppgiftsbiträde”, ”registrerad” och ”samtycke”.

Uppgifter som behandlas

Innovatum behandlar personuppgifter i första hand för att fullfölja Innovatums verksamhetsuppdrag och åtaganden. Utgångspunkten är att inte behandla fler personuppgifter än vad som behövs för ändamålet och Innovatum strävar alltid efter att använda de minst integritetskänsliga uppgifterna.

Inom ramen för sitt uppdrag behandlar, lagrar och överför Innovatum personuppgifter avseende deltagande i IBO´s, projekt, utställningar, pedagogiska program, aktiviteter och möten samt förtroendevalda såsom styrelseledamöter, valberedning, revisorer samt anställda och uppdragstagare.

Personuppgifter som behandlas är bland annat:

- personnummer
- namn, adress, telefonnummer, e-postadress
- fotografier
- bankrelaterade uppgifter (kontonummer, bankgironummer)
- arvode eller annan ersättning
- uppgift om innehållen skatt
- uppgift om arbetsgivaravgifter
- avtalsrelaterad information
- övrig frivilligt lämnad information i fritext via kontaktformulär eller liknande

Personuppgifterna behandlas i syfte att kunna fullgöra de förpliktelser och främja de syften som framgår av Innovatums stiftelseurkund, stadgar och styrdokument samt avtalade förpliktelser såsom att betala ut löner, arvoden och annan ersättning från Innovatum samt att ligga till grund för Innovatums löpande bokföring och redovisning. Vidare behandlas personuppgifterna i syfte att dokumentera och synliggöra Innovatums olika verksamhetsdelar i enlighet med stiftelseurkunden och därav fastställda styrdokument. Innovatum behandlar även personuppgifter för att kunna fullgöra lagstadgade förpliktelser såsom rapportering till myndigheter m.m.

Personuppgifter kan komma att uppdateras och kompletteras genom inhämtning från privata och offentliga register vid exempelvis uppdatering av adressuppgifter.

Överföring av personuppgifter

Inom ramen för Innovatum kan det bli nödvändigt att överföra eller koordinera personuppgifter avseende registrerade utanför Innovatums verksamhet.

Syftet med överföringen kan vara att Innovatum ska uppfylla skyldighet att rapportera till myndigheter eller andra för att uppfylla lagkrav eller för att uppfylla Innovatums åtagande enligt stiftelseurkunden och andra styrdokument. Överföring av personuppgifter utanför Innovatum ska begränsas till sådana uppgifter som är absolut nödvändiga för den aktuella åtgärden.

Personuppgiftsbiträde

Ett Personuppgiftsbiträde samt sådana personer som arbetar under Personuppgiftsbiträdets eller den Personuppgiftsansvariges ledning får enbart behandla personuppgifter i enlighet med instruktioner från Innovatum.

Om ett Personuppgiftsbiträde anlitas ska detta regleras i ett skriftligt avtal. Ett sådant avtal ska särskilt ange att Personuppgiftsbiträdet enbart får behandla personuppgifter i enlighet med instruktioner från Innovatum och att Personuppgiftsbiträdet ansvarar för att implementera lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

Grund för behandling

Innovatums behandling av personuppgifter grundas på samtycke från de registrerade samt behandling som är nödvändig för att fullgöra avtal i vilken den registrerade är part eller vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås. Vidare behandlas personuppgifter för att fullgöra rättsliga förpliktelser som åvilar Innovatum.

Information till registrerade i samband med att personuppgifterna lämnas

Information om hur personuppgifterna behandlas lämnas till de personer vars personuppgifter behandlas inom ramen för Innovatums verksamhet.

I första hand ges information när uppgifterna insamlas och den registrerade själv lämnar uppgifterna och samtycker till Innovatums behandling av dem.

Information till redan registrerade

Den registrerade har även att begära ut och få information om vilka personuppgifter om den registrerade som behandlas av Innovatum oberoende av hur dessa uppgifter har samlats in.

Om den registrerade vill ha sådan information ska han eller hon lämna in en skriftlig begäran till Innovatum. Begäran ska vara undertecknad av den registrerade samt skickas per post (e-post är således inte tillräckligt).

När någon ansökt om ett registerutdrag ska Innovatum i första hand lämna ett besked om huruvida personuppgifter som rör den sökande behandlas eller inte.

För det fall personuppgifter rörande den sökande behandlas ska Innovatum skriftligen lämna den sökande information om vilka personuppgifter som behandlas.
Informationen ska omfatta ändamålen med behandlingen, de kategorier av personuppgifter som behandlas, mottagare av personuppgifterna, lagringstid, möjligheten att begära rättelse eller radering av personuppgifterna, rätt att klaga hos tillsynsmyndighet och information om varifrån personuppgifter som den sökande själv inte lämnat kommer.

Den registrerade har även rätt till en kopia av de personuppgifter som är under behandling.

Om en registrerad begär information om sina personuppgifter ska Innovatum verka för att informationen lämnas utan onödigt dröjsmål och under alla omständigheter senast en månad efter att Innovatum har mottagit begäran.

Information till den registrerade ska på dennes begäran lämnas utan kostnad i vart fall en gång per kalenderår. Om personen i fråga onödigtvis belastar Innovatum med upprepade frågor som är uppenbart ogrundade och Innovatum kan bevisa det får Innovatum i undantagsfall vägra att lämna ut information.

Rättelse

Innovatum ska verka för att de personuppgifter som behandlas är korrekta.

Den registrerade har rätt att begära att dennes personuppgifter rättas, blockeras eller raderas om de är felaktiga eller om de behandlas i strid med gällande personuppgiftslagstiftning.

Säkerhet

Innovatum strävar efter att obehörig tillgång till personuppgifter inte kommer att ske. Innovatum försöker i största möjliga mån försäkra sig om att alla som behandlar Innovatums personuppgifter upprätthåller säkerheten avseende registrerade personuppgifter, lämplig teknologi och interna rutiner används för att undvika att obehöriga får tillgång till personuppgifter.

Innovatum vidtar lämpliga tekniska åtgärder för att skydda de personuppgifter som behandlas mot obehörig åtkomst, förstörelse och ändring. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, kostnaden för att genomföra åtgärderna, de särskilda risker som finns med behandlingen och hur känsliga personuppgifterna är.

Innovatum har även en förteckning över vilka som har åtkomst till uppgifterna.

Innovatum arbetar även för att säkerställa att det finns tekniska och praktiska förutsättningar att utreda eventuella misstankar om att någon haft obehörig åtkomst till personuppgifterna.

Lagring av personuppgifter

Personuppgifterna lagras bara så länge det är nödvändigt med hänsyn till ändamålet med behandlingen samt för att Innovatum ska kunna fullgöra sina skyldigheter enligt lag eller avtal.

Innovatum har rätt att lagra personuppgifter under den period då en tvist med en registrerad pågår eller för att fullgöra lagstadgade rapporteringar till myndigheter inklusive bevarandekrav.

Lagring och gallring av personuppgifter sker i enlighet med Innovatums dokumenthanteringsplan samt krav från Trollhättan stads stadsarkiv.

Personuppgiftsincident - riktlinjer

I dataskyddsförordningen definieras en personuppgiftsincident utifrån två perspektiv:

- En säkerhetsincident som leder till avsiktlig förstöring, förlust eller ändring av personuppgifter som behandlas
- En säkerhetsincident som leder till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som behandlas

Anmälan om personuppgiftsincident – allmänt

Datainspektionen är tillskyddsmyndighet för dataskydd och dit hörande integritetsfrågor och har till uppgift att utöva styrning, tillsyn och granskning av behandling av personuppgifter i Sverige.

Enligt Dataskyddsförordningen ska den personuppgiftsansvarige anmäla personuppgiftsincidenter till tillsynsmyndighet (förutsatt att den personuppgiftsansvarige beslutat och avgjort om vilken tillsynsmyndighet inom EU som organisationen ska rapportera personuppgiftsincidenter till). Om en personuppgiftsansvarig behandlar personuppgifter i flera länder, kan denne välja vilken tillsynsmyndighet inom ett EU-land som skall gälla för styrning, tillsyn, granskning och rapportering. I detta avseende är det också av betydelse för den personuppgiftsansvarige att bevaka nationell lag och rättsregler.

Hot och risker omfattar bland annat att den registrerade kan utsättas för bland annat:

- Diskriminering
- Bedrägeri (identitetsstöld, finansiell förlust, ryktesspridning samt brott mot sekretess eller tystnadsplikt).

Anmälan

Den personuppgiftsansvariges anmälan om personuppgiftsincident syftar till att:

- En tillsynsmyndighet ska kunna granska befintliga och vidtagna åtgärder en organisation genomfört avseende behandling av personuppgifter samt
- Bevaka vilka ytterligare åtgärder som vidtas, för att motverka fortsatta och negativa effekter av en personuppgiftsincident
- Om det blir nödvändigt, kan tillsynsmyndighet komma att utöva sina tillsynsbefogenheter för att få den som är personuppgiftsansvarig att vidta nödvändiga skyddsåtgärder, om befintliga åtgärder anses för vaga eller otillräckliga

En personuppgiftsincident ska anmälas till tillsynsmyndighet 72 timmar från det att en personuppgiftsincident skett. Om det är omöjligt för den personuppgiftsansvarige att lämna all information inom 72 timmar, kan den personuppgiftsansvarige meddela relevanta uppgifter till tillsynsmyndigheten vid olika tillfällen allt eftersom det är möjligt. Den personuppgiftsansvarige ska ändå informera tillsynsmyndigheten om skäl till uppdelning eller försening gällande anmälan om personuppgiftsincident.