1. Formalia

1.1 Sammanfattning

Denna policy reglerar vad som gäller vid personuppgiftshantering inom Stampus.

1.2 Syfte

Syftet med detta direktiv är att Stampus styrelse, medlemmar samt projekt och utskott skall veta vad som gäller vid hantering och lagring av personuppgifter. Dokumentet skall fungera som ett stöd till Stampus personuppgiftshantering och hjälpa organisationen att följa riktlinjerna i Dataskyddsförordningen.

1.3 Omfattning

Detta direktiv gäller för samtliga medlemmar i Stampus.

1.4 Spridning

Samtliga aktiva ska vid tillträde informeras om rådande dataskyddspolicy och rutiner för hantering av personuppgifter. Det är styrelsen som är ytterst ansvarig att säkerställa att detta görs.

2. Vad är Dataskyddsförordningen?

2.1 Generell information

Dataskyddsförordningen (engelska: General Data Protection Regulation eller GDPR) är en EU-förordning som träder i kraft den 25 maj 2018. Förordningen byter ut den nationella Personuppgiftslagen (PUL) som Sverige tidigare har haft. Mycket är sig likt, men förordningen ställer tuffare krav på organisationer som samlar in och behandlar personuppgifter. Straffen för de som bryter mot förordningen är tuffare än de var för de som bröt mot Personuppgiftslagen: organisationer som bryter mot Dataskyddsförordningen kan få betala en administrativ sanktionsavgift på upp till 20 miljoner euro eller 4 % av deras 3 totala årliga omsättning (beroende på vilket som är högst). I Sverige är det Datainspektionen som tar beslut i sådana frågor. Datainspektionen har under Dataskyddsförordningen makt att granska vilken organisation som helst i Sverige, utan att tidigare informera om att en granskning ska göras. Man kan även anmäla organisationer till Datainspektionen, som då kan välja att göra en granskning. Om Datainspektionen kontaktar en organisation och vill göra en granskning måste organisationen kunna visa dokumentation på hur Dataskyddsförordningen följs, utan dröjsmål.

2.2 Dataskyddsförordningens syfte

Dataskyddsförordningens syfte är att skydda enskilda individers privatliv och personuppgifter, säkerställa att organisationer som behandlar personuppgifter gör detta på ett korrekt och säkert sätt, samt att se till att skyddet som ges håller samma nivå i hela Europeiska Unionen. Syftet är också att ersätta de direktiv som funnits tidigare, vilka beskrivits som ”tandlösa” och omoderna.

3. Lagring av personuppgifter

3.1 Vad är en personuppgift?

Dataskyddsförordningen definierar en personuppgift som ”varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet”.

Med andra ord är en personuppgift allt som kan kopplas till en specifik person. Detta inkluderar namn, mejladresser, personnummer och bilder

3.2 Personuppgiftsförteckning

För att enkelt kunna informera om vilka personuppgifter Stampus samlar in samt hur och till vilka ändamål dessa används (något som dataskyddsförordningen ställer krav på) behövs en personuppgiftsförteckning. Förteckningen ska innehålla information om:

- Vilka personuppgifter Stampus samlar in
- Vad dessa personuppgifter används till
- Vem som är ansvarig för hanteringen av personuppgifterna (detta är Stampus som organisation, då vi inte har ett dataskyddsombud), samt kontaktuppgifter till denne
- Vilka kategorier av personer som har personuppgifter registrerade (i Stampus fall inkluderar detta exempelvis ”medlemmar” och ”aktiva medlemmar”)
- Tidsgräns för borttagning av personuppgifter (se kapitel 4.4)
- Beskrivning av säkerhetsrutiner kring personuppgiftshantering

3.3 Samtycke

Samtycke behövs i de allra flesta fall då personuppgifter ska samlas in och behandlas. Dataskyddsförordningen förtydligar att detta samtycke ska ske genom en ”entydig bekräftande handling”. Samtycket ska vara ett ”frivilligt, specifikt, informerat och otvetydigt medgivande”. Detta innebär exempelvis att tystnad, inaktivitet och i förväg ikryssade rutor i ett formulär inte kan ses som samtycke. När samtycke inhämtas ska tydlig information ges till personen ifråga om vilka personuppgifter som kommer samlas in, varför dessa samlas in och hur de kommer användas. Det är viktigt att man kan dokumentera att samtycke för personuppgiftsbehandling har getts. Dokumentation av det här slaget måste alltså sparas och hållas lättillgängligt.

Personuppgifter som samlas in får endast användas i det syfte som berörda personer har gett sitt samtycke till. Notera även att man vid insamling av personuppgifter ska arbeta utefter dataminimeringsprincipen. Denna innebär att man endast ska samla in de personuppgifter man behöver ha, vilket kan summeras i frasen ”need to know, not nice to know.”

3.4 Bilder och marknadsföringsmaterial

Som tidigare nämnts kan även bilder ses som personuppgifter, om det är möjligt att identifiera specifika individer i dessa bilder, antingen i sig själva eller genom att jämföra med

andra bilder. Detta innebär att samtycke måste hämtas in vid fotografering av privatpersoner. Det är viktigt att man specificerar hur bilderna kommer behandlas – alltså om de kommer läggas ut på sociala medier, på en hemsida, eller sparas i en databas – när man inhämtar samtycke. Företrädesvis bör man ha formulär på plats när foton ska tas, som beskriver hur bilderna kommer användas och tydligt ber om samtycke. Alternativt kan man spela in en muntlig överenskommelse. Undantag gäller för vimmelbilder – se längre ner i detta stycke. Förordningen gäller även för gamla bilder. Så länge bilderna kan användas för att identifiera en nu levande person så behövs det ett otvetydigt samtycke från denne. Bilder som inte har fått ett sådant samtycke måste raderas, både där de finns publicerade och där de finns sparade i eventuella databaser. Vill man använda bilder för att ta fram marknadsföringsmaterial i form av broschyrer, affischer eller liknande, behöver man få samtycke specifikt för denna behandling.

Enligt Datainspektionen bör samtycke ej användas som den rättsliga grunden för publicering av mingelbilder, då detta kan bli onödigt krångligt. Däremot kan man använda sig av en annan rättslig grund, nämligen en intresseavvägning. Detta kan göras när syftet med publiceringen är att informera om verksamheten och man bedömer att intresset för detta väger tyngre än intresset personerna på bilderna har av att skydda sina personuppgifter. När man gör en intresseavvägning av den här sorten ska det dokumenteras. Det är också viktigt att komma ihåg de rättigheter som personerna på bilderna har. Därför ska besökarna på evenemang och liknande informeras om att de kan hamna på bild och att dessa bilder kan användas för att informera om verksamheten. De måste också få information om att de har möjlighet att invända mot detta och vem de ska kontakta för att göra det. Ovanstående gäller endast i de fall man vill använda mingelbilder för att informera om verksamheten. I de fall man vill använda mingelbilder i marknadsföringssyfte gäller strängare regler. För att använda personers namn och/eller avbildning i marknadsföringsmaterial krävs explicit samtycke.

3.5 De registrerades rättigheter

De vars personuppgifter som Stampus samlar in och behandlar har ett antal rättigheter som måste respekteras. För en fullständig redogörelse av de registrerades rättigheter, se Dataskyddsförordningen. Några av de mest relevanta rättigheterna för vår verksamhet ser ut så här:

- Rätten att bli bortglömd. Detta innebär att en person kan begära att alla deras personuppgifter ska raderas från våra system, databaser och publiceringsplattformar. Även back-upp kopior på dessa personuppgifter måste då tas bort.
- Rätten till dataportabilitet. Detta innebär att en person kan begära att få en kopia på alla sina personuppgifter som finns sparade av Stampus i ett format som tillåter dem att enkelt överföra dem till en annan personuppgiftsansvarig. En sådan begäran ska tillgodoses inom en månad, utan kostnad för den registrerade. 6
- Rätten till rättelse. Detta innebär att en person kan begära att få sina personuppgifter rättade om de innehåller felaktigheter. Detta ska ske utan onödigt dröjsmål.
- Personuppgifter som samlas in får endast användas i det syfte som berörda personer har gett samtycke till.

4. Säkerhetsrutiner

4.1 Var sparas personuppgifter?

Det åligger den personuppgiftsansvarige – Stampus styrelse– att ta rimliga säkerhetsåtgärder för att säkerställa att ingen utomstående får åtkomst till insamlade personuppgifter. Ett led i detta är att förvara personuppgifter på ett tryggt sätt. Alla personuppgifter som vår organisation samlar in ska förvaras digitalt, i vår Google Drive. Google har ett tillräckligt högt intrångsskydd för att detta ska vara acceptabelt, då de innehar en Privacy Shield-certifiering. Dock måste vissa säkerhetsrutiner vidtas även här. Samtliga styrelsemedlemmar ska uppdatera sina inloggningsuppgifter när de stiger på. De ska alltså inte ha samma användarnamn och lösenord som sin företrädare. Om de är inloggade på Driven i sina mobila enheter ska dessa enheter vara låsta med en säkerhetskod. Om en styrelsemedlem blir bestulen på sin mobil och/eller dator, ska denne omedelbart uppdatera sina inloggningsuppgifter och informera Stampus ordförande om händelsen. I vissa fall kommer vi ha personuppgifter insamlade i pappersformat. Detta kan inkludera kvittopapper och formulär. Dessa måste överföras digitalt till vår Drive så fort som möjligt och därefter ska pappersversionerna makuleras. Under tiden de finns sparade i pappersformat måste de hållas otillgängliga för utomstående, företrädesvis på Stampus kontor på Borgen och inlåsta i ett skåp.

4.2 Personuppgifter på mejlen

När Dataskyddsförordningen träder i kraft försvinner den så kallade ”missbruksregeln”. Denna innebar tidigare att man kunde använda enklare regler för personuppgifter i ostrukturerat material. Med ostrukturerat material menas bland annat e-post och inlägg i sociala medier. När missbruksregeln försvinner gäller samma regler även för personuppgifter i ostrukturerat material. Detta innebär att vi som organisation måste ha tydliga rutiner kring hur vi hanterar personuppgifter i vår mejl. E-post innebär i princip alltid personuppgiftshantering, eftersom själva epostadressen i de flesta fall är en personuppgift i sig. All information i ett mejl som kan kopplas till en specifik person är också en personuppgift. Det är innehållet i mejlen som avgör om och hur länge den sparas. Man ska exempelvis i största möjliga mån undvika att skicka eller ta emot mejl som innehåller så kallade känsliga personuppgifter; detta kan exempelvis vara uppgifter om en persons hälsa. Om någon verksam inom Stampus tar emot ett mejl med känsliga personuppgifter ska denna raderas så fort som möjligt. Även papperskorgen ska rensas. För att undvika att gamla mejl med personuppgifter finns kvar i inkorgen behövs tydliga raderingsrutiner. Se 4.4 för dessa.

4.3 Tillgång till personuppgifter och personuppgiftsincidenter

För att ha en hög nivå på säkerheten kring vår personuppgiftshantering ska tillgång till personuppgifterna vi behandlar begränsas i största möjliga mån. Endast de som har behov av personuppgifterna ska ha tillgång till dem. Om personuppgifter som vi behandlar förstörs, går förlorade eller hamnar i orätta händer kallas detta för en personuppgiftsincident. Personuppgiftsincidenter ska anmälas till Datainspektionen inom 72 timmar efter att de har

upptäckts. Berörda personer ska kontaktas och informeras omedelbart om incidenten utgör en risk för att deras rättigheter och friheter påverkas.

4.4 Raderingsrutiner

Personuppgifter ska inte sparas längre än nödvändigt. Tumregeln här är att personuppgifter ska raderas när de inte längre behövs för att fylla det syfte de samlades in för. Register över utskottsmedlemmar ska uppdateras årligen och medlemmar som lämnat utskottet ska då tas bort. Om en utskottsmedlem kontaktar den utskottsansvarige och meddelar att de ämnar att lämna utskottet ska deras personuppgifter tas bort omedelbart. Personuppgifter för studentrepresentanter, projektmedlemmar, valberedning samt styrelse och revisorer ska raderas när de har fullgjort sin förtroendeperiod. Om de väljer att lämna sin post innan denna period löper ut, ska deras personuppgifter tas bort omedelbart.

Bilder från evenemang som tagits för mer än två år sedan ska raderas. Undantag kan göras för bilder som har ett historiskt värde, exempelvis bilder på projektgrupper och styrelser eller från särskilt viktiga evenemang. Mejl som innehåller personuppgifter (utöver e-postadressen) ska raderas så fort som möjligt. Vid slutet av varje aktiv medlems uppdrag ska deras inkorg rensas. Alla mejl som inte behövs för att driva verksamheten ska då raderas och papperskorgen ska tömmas. Om någon inom organisationen tar emot ett mejl som ska vidarebefordras (för att mottagaren ej kan besvara den), ska detta mejl raderas omedelbart efter vidarebefordring. Omedelbart efter detta ska även papperskorgen rensas. Officiella Stampus-mejlkonton samt personliga mejlkonton som används i Stampus syfte ska avslutas med en fotnot innehållande följande text: ”Ditt mejl kan komma att sparas under en period. För information om hur vi behandlar personuppgifter besök länk till dataskyddspolicy på hemsidan”. För mer utförlig information om samtliga raderingsrutiner och andra rutiner relaterade till vårt dataskyddsarbete, se dokumentet ”Rutiner för hantering av personuppgifter”. i