



NEWMANINSTITUTET
HÖGSKOLA FÖR TEOLOGI, FILOSOFI OCH KULTUR

Dokumentstyp: Policydokument

Beslutsfattare: Högskolestyrelsen

Beslutsdatum: 2022-09-07

Reviderad: 2023-08-30

Dokumentansvarig: Högskoledirektör.

Dataskydds- och informationssäkerhetspolicy vid Newmaninstitutet





Innehållsförteckning

<i>Inledning – generella riktlinjer.....</i>	<i>3</i>
<i>Definitioner och begrepp.....</i>	<i>3</i>
Personuppgiftsansvarig (PUA).....	3
Personuppgiftsbiträde (PUB)	4
Personuppgiftsbiträdesavtal	4
Personuppgifter	4
Känsliga personuppgifter	5
Laglig grund för behandling av personuppgifter.....	6
Personuppgiftsincident.....	7
<i>Hantering av personuppgifter på Newmaninstitutet.....</i>	<i>7</i>
Ansvar	7
Cookies	8
E-post	6
Personuppgifter NI hanterar för Anställd	8
Personuppgifter NI hanterar för Student.....	9
Personuppgifter inom ramen för forskningsprojekt	10
Personuppgifter som NI hanterar för deltagare i aktivitet eller enkäter.....	10
<i>Registrerades rättigheter</i>	<i>11</i>
<i>Hantering av personuppgiftsincident.....</i>	<i>11</i>

Inledning – generella riktlinjer

Det finns lagar och förordningar på dataskyddsområdet som tillkommit för att skydda den enskilda medborgarens personliga integritet¹ och Newmaninstitutet (NI) som personuppgiftsansvarig är ansvariga för att lagstiftningen följs och att kontinuerligt arbeta för att förebygga personuppgiftsincidenter. Det är också av vikt för NI att de som berörs av hantering av personuppgifter känner tillit och trygghet med vår hantering. NI ska därför vara öppna med hur NI behandlar personuppgifter dvs hur vi samlar in, registrerar, strukturera, lagrar, gallrar, arkiverar och i förekommande fall delar den information som sparats.

En grundregel vid NI är att *inte samla in, registrera och strukturera fler personuppgifter än vad som är nödvändigt*, vilket innebär att alla medarbetare har ett ansvar att beakta behov av insamling av personuppgifter och att endast personuppgifter centrala för uppdraget och verksamheten ska samlas in och användas. En annan grundregel är att *personuppgifter inte ska sparas längre än nödvändigt*, vilket innebär att alla medarbetare har ett ansvar att gallra eller avidentifiera de personuppgifter som samlats in så snart det inte längre finns skäl eller ändamål med att spara personuppgifterna. En tredje grundregel är att NI *ska hantera informationen på ett systematiskt och informationssäkert sätt* för att säkerställa tillgänglighet, riktighet och att endast behöriga personer kan ta del av informationen som finns sparad.

För behandling av personuppgifter och annan information som är känslig för verksamheten är det viktigt att varje medarbetare hanterar dessa med gott omdöme och iaktta särskild försiktighet för att förebygga och därmed undvika risker för exempelvis personuppgiftsincidenter eller att (för verksamheten känslig) information kommer i orätta händer.

Definitioner och begrepp

Personuppgiftsansvarig (PUA)

Personuppgiftsansvarig är normalt den juridiska person (till exempel aktiebolag, stiftelse, förening eller myndighet) som bestämmer vilka personuppgifter som ska behandlas i

¹ Framför allt den europeiska dataskyddsförordningen/GDPR och den svenska dataskyddslagen som utgör ett komplement till den förnämnda



NEWMANINSTITUTET

HÖGSKOLA FÖR TEOLOGI, FILOSOFI OCH KULTUR

verksamheten och vad uppgifterna ska användas till. Personuppgiftsansvarig är skyldig att föra register över behandlingar och vidta lämpliga säkerhetsåtgärder för att skydda de uppgifter som behandlas. NI är i dessa sammanhang personuppgiftsansvarig.

Personuppgiftsbiträde (PUB)

Personuppgiftsbiträde är normalt den juridiska person (till exempel aktiebolag, stiftelse, förening eller myndighet) som behandlar personuppgifter för den personuppgiftsansvariges, i detta fall NI:s, räkning exempelvis för hantering av anställdas löner eller en molntjänstleverantör. Personuppgiftsansvaret kan aldrig överlåtas utan arbetsgivaren är fortsatt ansvarig för behandling som utförs av PUB.

Personuppgiftsbiträdesavtal

Ett skriftligt avtal mellan arbetsgivaren (i detta fall NI) som personuppgiftsansvarig och personuppgiftsbiträdet. Där ska bland annat framgå att personuppgiftsbiträdet, inklusive dess anställda, bara får behandla personuppgifter i enlighet med överenskomna avtal eller dokumenterade instruktioner från den personuppgiftsansvariga och att biträdet ska bistå den personuppgiftsansvariga på olika sätt. Det är alltså arbetsgivaren (i detta fall NI) som bestämmer för vilka ändamål personuppgifterna får behandlas. Personuppgiftsansvarig är skyldig att föra register över behandlingar och att vidta lämpliga säkerhetsåtgärder för att skydda de uppgifter som behandlas.

Personuppgifter

Personuppgifter är all information som direkt eller indirekt kan knytas till en person som är i livet. Typiska personuppgifter är personnummer, namn och adress. Även foton på personer klassas som personuppgifter. Ett organisationsnummer är en personuppgift om det handlar om en enskild firma. Registreringsnumret på en bil är en personuppgift om det går att knyta till en person, medan registreringsnumret på en firmabil som används av flera anställda, inte är en personuppgift. I vissa fall räknas även olika slags elektroniska identiteter, som exempelvis ip-adress, som personuppgifter om de kan kopplas till en viss person.



NEWMANINSTITUTET

HÖGSKOLA FÖR TEOLOGI, FILOSOFI OCH KULTUR

Behandling av personuppgifter

För att få behandla² personuppgifter måste det finnas stöd i dataskyddsförordningen och personuppgifter får endast samlas in för specifika, särskilt angivna och berättigade ändamål.

Behandling av personuppgifter är således förbjuden enligt dataskyddsförordningen (GDPR) om den inte uppfyller kraven som finns angivna i förordningen.

De krav som behandling av registrerade och strukturerade personuppgifter ska följa är först och främst att det ska finnas dokumenterade ändamål och laglig grund för behandlingen – dokumentet i sammanhanget är behandlingsregistret enligt GDPR artikel 30. Man får inte heller behandla personuppgifter för andra ändamål än de ändamål för vilka uppgifterna initialt samlats in.

GDPR är teknikneutral, d.v.s. det spelar ingen roll om personuppgifterna finns i ett datasystem eller i en pärm. T.ex. styrs personuppgifter som finns sorterade i en pärm med register av GDPR, men inte personuppgifter i lösa anteckningar eller elektroniska minnesanteckningar i mapp på datorn. Även en e-postlåda är ett register i GDPR:s mening om personuppgifterna där registreras, struktureras och lagras.

I enlighet med GDPR:s artiklar 5 och 6 gäller dessutom följande 7 grundläggande principer för att organisationen ska ha rätt att behandla personuppgifter:

1. Laglighet, korrekthet/rimlighet och öppenhet
2. Ändamålsbegränsning
3. Uppgiftsminimering
4. Korrekthet
5. Lagringsminimering
6. Integritet och konfidentialitet
7. Ansvarsskyldighet

Känsliga personuppgifter

I dataskyddsförordningen/GDPR skiljer man mellan vanliga personuppgifter och känsliga personuppgifter³. Med känsliga personuppgifter menas bland annat: etnisk ursprung, politiska

² Behandla är ett vitt begrepp som innebär att göra något med en personuppgift exempelvis samla in, registrera, strukturera, lagra, gallra eller arkivera personuppgifter

³ Läs mer i artikel 9 i General Data Protection Regulation (GDPR).



NEWMANINSTITUTET

HÖGSKOLA FÖR TEOLOGI, FILOSOFI OCH KULTUR

åsikter, religionsåskådning eller sexuell läggning. Även uppgifter om personens hälsa och om personen tillhör en fackförening klassas som känsliga. Dessa är förbjudna att behandla om inte särskilda förutsättningar föreligger.

Laglig grund för behandling av personuppgifter

Det finns sex lagliga grunder för behandling av personuppgifter:

Samtycke: När en person skriftligen har lämnat sitt samtycke till att personuppgifter behandlas för ett eller flera specifika ändamål. Nackdelen med samtycke är att det är individuellt när som helst kan återtas helt eller delvis. Samtycke ska därför användas i sista hand, då ingen annan grund för behandling finns. Om behandlingen kräver samtycke, ska samtycke inhämtas innan behandlingen av personuppgifter påbörjas.

Avtal: Om uppgifterna är nödvändiga för att fullgöra ett avtal, exempelvis anställningsavtal, kundavtal, hyresavtal, leverantörsavtal

Rättslig förpliktelse: Om uppgifterna är nödvändiga för att fullgöra en laglig skyldighet, t.ex. bokföringsskyldigheten i bokföringslagen

Intressevägning: Om det finns ett berättigat behov av att hantera uppgifterna och att detta behov väger tyngre än den enskildas rätt till skydd

Myndighetsutövning och uppgifter av allmänt intresse: Om den personuppgiftsansvariga måste behandla personuppgifter för att utföra sina myndighetsuppgifter eller för att utföra en uppgift av allmänt intresse

Grundläggande intresse: Om den personuppgiftsansvariga måste behandla personuppgifter för att skydda en registrerad som inte kan lämna samtycke, till exempel om hen är medvetlös eller vid "force majeure" -situationer

Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som kan innebära risk för människors frihet och rättighet. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Exempel:

- diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning
- ekonomisk förlust
- brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har

- blivit förstörda
- gått förlorade på annat sätt
- kommit i orätta händer.

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

Hantering av personuppgifter på Newmaninstitutet

NI ska inte samla in fler personuppgifter än vad som är nödvändigt, uppgifterna ska inte sparas längre än nödvändigt och informationen ska hantera på ett systematiskt och informationssäkert sätt för att säkerställa tillgänglighet, riktighet och att endast behöriga personer kan ta del av informationen som finns sparad. Hur olika personuppgifter ska behandlas ska framgå av NI:s interna rutiner. Finns frågor kring NI:s behandling av personuppgifter ska högskoledirektör vid NI kontaktas.

Ansvar

Newmaninstitutet AB (org.nr 556563-8128) styrelse är juridiskt sett högsta är personuppgiftsansvarig instans. Rektor och respektive områdesansvarig funktion/roll har det övergripande ansvaret för hantering av personuppgifter i enlighet med detta styrdokument och gällande lagstiftning. Alla medarbetare har ett ansvar att följa detta styrdokument och gällande lagstiftning. Eventuella personuppgiftsbiträdesavtal och arkivering följer detta styrdokument. Vid behov kan separata rutiner tas fram för hantering och arkivering för specifika områden exempelvis forskningsprojekt.



Cookies

På NI:s hemsida www.newman.se används cookies för att optimera webbsidans funktion.

Cookies används inte för att identifiera individ, genomföra analys, ge underlag till riktad annonsering eller profilering av annat slag och personuppgifter hanteras och lagras därmed inte vid användning av NI:s externa hemsida. Mer information om vilka cookies som används och hur de hanteras återfinns i NI:s Cookie policy⁴ tillgänglig på Newmaninstitutets hemsida.

Personuppgifter NI hanterar för Anställd

När någon blir, är eller har varit anställd vid NI hanteras:

- Uppgifter som medarbetaren själv lämnar såsom namn, personnummer och kontaktuppgifter, inklusive telefonnummer och e-postadress
- Kontaktuppgifter till närmast anhörig (kontaktperson)
- Kontouppgifter för löneutbetalning
- Uppgifter om försäkringar
- Sjuk/läkarintyg

I förekommande fall kan också följande hanteras:

- Bilder på NI server och hemsida
- Uppgifter i samband med tillbudsrapportering eller liknande interna ärenden.

Rättslig grund för hanteringen:

- Personuppgifterna hanteras med stöd i *samtycke* samt *fullgörande av avtal* för att administrera anställningen hos NI och *intressevägning* för arkivering av bilder för historiedokumentation.

Överföring av personuppgifter:

- Vissa personuppgifter kan vid behov delas med personuppgiftsbiträden såsom leverantörer av IT-system, rapportering till SCB, Skatteverket, försäkringar, Erasmus (personalmobilitet) eller löneadministration.

Lagringstid:

- Personuppgifterna sparas under anställningen och därefter i upp till 7 år
- Personuppgifter som hanteras inom ramen för personalmobilitet inom Erasmus sparas i 3 år
- Namn, personnummer och anställningstid raderas inte.

⁴ <https://newman.se/cookie-policy-eu/>



NEWMANINSTITUTET

HÖGSKOLA FÖR TEOLOGI, FILOSOFI OCH KULTUR

Personuppgifter NI hanterar för Student

När någon blir, är eller har varit student vid NI hanteras:

- Uppgifter som studenten själv lämnar direkt till NI eller via antagningen.se (som hanteras av Universitets – och högskolerådet) såsom namn, personnummer och kontaktuppgifter, inklusive telefonnummer och e-postadress
- I förekommande fall personuppgifter från andra lärosäten om studenten studerat tidigare
- I förekommande fall personuppgifter som lämnas i samband med utbytesstudier/Erasmusstudier
- Studieresultat och annan information om studierna, exempelvis examinationer

I förekommande fall kan också nedan hanteras:

- Bilder på server, hemsida eller kurskatalog
- Sjuk/läkarintyg
- Uppgifter om särskilda behov
- Uppgifter i samband med tillbudsrapportering eller andra interna ärenden

Rättslig grund för hanteringen:

- Personuppgifterna hanteras med stöd i *myndighetsutövning och uppgifter av allmänt intresse* (som led i NI:s uppdrag som enskild utbildningsanordnare), *intressevägning* och *samtycke* samt *rättslig förpliktelse*.

Överföring av personuppgifter:

NI kan i vissa fall komma att överföra personuppgifter till andra organisationer, exempelvis:

- Andra högskolor i Sverige eller utomlands exempelvis vid tillgodoräknanden eller utbytesstudier
- CSN för beviljande och utbetalning av studiestöd
- SCB och utbildningsdepartementet för att skapa officiell statistik

Lagringstid:

- Samtliga personuppgifter sparas under studierna och därefter i upp till 2 år
- Personuppgifter som hanteras i samband med Erasmusstudier sparas i 3 år
- Namn, personnummer och betyg på genomförda kurser/ utbildningsprogram liksom examensbevis raderas inte
- Kontaktuppgifter till studenter och alumner sparas för att kunna hantera utskick av studentenkät och alumnenkät liksom inbjudningar till alumni-nätverket



NEWMANINSTITUTET

HÖGSKOLA FÖR TEOLOGI, FILOSOFI OCH KULTUR

Personuppgifter inom ramen för forskningsprojekt

När någon deltar eller har deltagit i ett forskningsprojekt hanteras:

- De uppgifter som källan själv angett inom ramen för projektet vilket kan vara namn, adress eller andra kontaktuppgifter
- De uppgifter som krävs för att forskaren ska kunna genomföra forskningsprojektet, för hantering och arkivering i enlighet med god forskningssed se styrdokumentet Riktlinjer om forskning

Rättslig grund för hanteringen:

- Personuppgifterna hanteras med stöd i *samtycke*

Lagringstid:

- Personuppgifterna anonymiseras skyndsamt av respektive forskare och endast anonymiserat material arkiveras

Personuppgifter som NI hanterar för deltagare i aktivitet eller enkäter

I samband med events (seminarier, föreläsningar, inspelning av podcasts, filmade intervjuer, konferenser etc.) eller i samband med undersökningar (enkäter och intervjuer) hanteras de uppgifter som deltagaren eller respondenten lämnar inklusive namn och kontaktuppgifter.

Personuppgifterna hanteras för att:

- Administrera aktiviteten och för att kunna återkoppla till deltagaren/respondenten
- Skapa reportage och annat material för sändning
- Ge god service
- Hantera födoämnesallergier i samband med förtäring (OBS att detta är känsliga personuppgifter, eftersom det rör individens hälsa).
- Ta fram statistik i syfte att förbättra verksamheten

Rättslig grund för hanteringen:

- Personuppgifterna hanteras som stöd i *intresseavvägning* och även *fullgörande av avtal* vid aktiviteter som sker i samarbete med andra. För föreläsare och andra deltagare vid event som spelas in hanteras personuppgifter med stöd i *samtycke*. Hantering av personuppgifter som rör födoämnesallergier bör hanteras utifrån den lagliga grunden Samtycke.

Lagringstid:

- Personuppgifter i relation till anmälan och deltagande sparas inte längre än sex månader från att aktiviteten eller enkäten genomförts



NEWMANINSTITUTET

HÖGSKOLA FÖR TEOLOGI, FILOSOFI OCH KULTUR

- Material som skapas från event, exempelvis ljudfiler eller videoinspelningar, sparas efter samtycke i arkiv tillgängligt via hemsidan.

Registrerades rättigheter

Alla registrerade har rätt att:

- Få information och ett registerutdrag över vilka personuppgifter som behandlas. Den registrerade har också rätt till tillgång, vilket innebär rätt att få ut själva personuppgifterna i ett format som är av sådant slag att den registrerade själv kan kontrollera personuppgifternas riktighet.
- Vända sig till NI och be att få sina personuppgifter raderade, rättade eller kompletterade. Det finns dock undantag till rätten till radering till exempel för att utföra en uppgift av allmänt intresse vilket innebär att en sådan begäran inte alltid kan tillmötesgå
- Begära att behandlingen av deras personuppgifter begränsas
- Invända mot behandlingen av personuppgifter
- Inte bli föremål för automatiserat beslutsfattande och profilering
- Kunna få ut inlämnade personuppgifter i ett format som möjliggör dataportabilitet
- Vid missnöje över NI:s hantering av personuppgifter anmäla detta till Integritetsskyddsmyndigheten (IMY) som är ansvarig tillsynsmyndighet

Hantering av personuppgiftsincident

Misstanke

Om medarbetare vid NI misstänker att personuppgiftsincident har inträffat så ska detta rapporteras till högskoledirektör eller berörd områdesansvarig. Det är berörd områdesansvarig som tillsammans med medarbetaren utreder huruvida personuppgiftsincident har inträffat.

Bekräftad incident

Om en medarbetare vid NI får kännedom om att personuppgiftsincident har inträffat så ska detta direkt meddelas till högskoledirektör eller berörd områdesansvarig. Det är berörd områdesansvarig som ansvarar för att säkerställa att rektor snarast möjligt informeras om personuppgiftsincidenten. Områdesansvarig ansvarar också för att tillsammans med rektor



NEWMANINSTITUTET

HÖGSKOLA FÖR TEOLOGI, FILOSOFI OCH KULTUR

och medarbetaren utreda huruvida personuppgiftsincidenten utgör en risk för fysiska personers friheter och rättigheter.

Risk för fysiska personers friheter och rättigheter

Vid personuppgiftsincident som utgör risk för fysiska personers friheter och rättigheter ska berörd områdesansvarig anmäla incidenten till Integritetsskyddsmyndigheten (IMY)/tillsynsmyndighetens e-tjänst inom 72 timmar från upptäckt. Det är möjligt att lämna kompletterande uppgifter inom fyra veckor. Efter anmälan ska de lämpliga åtgärder⁵ som identifieras under utredningen antingen genomföras eller läggas in i en handlingsplan. Om personuppgiftsincidenten bedöms kunna leda till en hög risk för de registrerades friheter och rättigheter ska de registrerade informeras.

Ingen risk för fysiska personers friheter och rättigheter

Vid personuppgiftsincident som inte utgör risk för fysiska personers friheter och rättigheter ska berörd områdesansvarig skriva en incidentrapport, som beskriver händelsen, omständigheterna, dess effekter och de åtgärder som vidtagits. Incidentrapport kan med fördel noteras direkt i Daylite med rubriken personuppgiftsincident. Om incidentrapporten innehåller känslig information kan ovan information sammanställas i ett dokument som skickas till högskoledirektör för arkivering.

Dokumentation av personuppgiftsincidenter

NI ska arkivera alla incidentrapporter och ska kunna uppvisa dem för Integritetsskyddsmyndigheten (IMY), som är ansvarig tillsynsmyndighet, vid eventuell tillsyn.

⁵ Exempel på lämpliga åtgärder kan vara upprättande eller förbättrande av en dokumenterad rutin, rätta till bugg i datasystem eller avidentifiera personuppgifter som inte är nödvändiga att behandla.