	Författare/Issuer: Karin Liljebadh	Kontrollerad av/Controlled by: Johan Eriksson	Dok. nr./doc. Nr.:
	Utgåva/datum: 3/210826	Ersätter: 2/181218	Sida: 1/5
Dokumentnamn: <p style="text-align: center;">INTEGRITETSSKYDDSPOLICY</p>			

Kvalitet, Säkerhet & Miljö

Inledning

Den personliga integriteten är viktig för NordArom AB (nedan kallat NordArom). Detta dokument beskriver hur medarbetare på NordArom skall arbeta för att säkerställa att den personliga integriteten är skyddad.

Definitioner

Dataskyddsförordningen (GDPR) är EU-förordningen som ersätter PUL (personuppgiftslagen).

Personuppgifter är alla uppgifter och information som rör en individ. Det kan vara allt från namn, bilder, e-postadress, bankkontonummer till IP-adress, CV och betyg.

Personuppgiftsbehandling är all behandling av personuppgifter, t.ex. insamling, lagring och läsning.

Samtycke är ett skriftligt eller muntligt godkännande från individ, där individ uttryckligen samtycker till personuppgiftsbehandling.

Integritetsskyddsmyndigheten (IMY) är en myndighet som genom sin tillsynsverksamhet ska bidra till att behandlingen av personuppgifter inte leder till otillbörliga intrång i enskilda individers personliga integritet.

Rättslig grund betyder att NordArom har rätt till personuppgiftsbehandlingen, behandlingen är laglig.

Dataskyddsombudet (DSO) är den som säkerställer att NordArom arbetar enligt nedan riktlinjer och dataskyddsförordningen (GDPR). Lukas Aldén är utsedd till NordAroms dataskyddsombud.


Omfattning

Denna integritetsskyddspolicy gäller för alla medarbetare på NordArom, såväl fulltids- som deltidsanställda.

Grundläggande principer

NordArom AB ska vidta alla rimliga åtgärder för att säkerställa att skyddet för den personliga integriteten är starkt inom företaget. Det gäller såväl behandlingen av personuppgifter om prospekter, kunder, leverantörer, kandidater och internanställda, och alla andra individer som kan komma att registreras i NordAroms register och IT-system. All personuppgiftshantering på NordArom ska ske i enlighet med dataskyddsförordningen (GDPR). Det innebär att NordAroms medarbetare skall behandla personuppgifter korrekt och endast för att utföra sina arbetsuppgifter.

För att uppnå ett bra integritetsskydd ska NordArom inte bara se till att personuppgifter skyddas av teknik. Det är minst lika viktigt att kontinuerligt arbeta med frågor så som lojalitet,

	Författare/Issuer: Karin Liljebladh	Kontrollerad av/Controlled by: Johan Eriksson	Dok. nr./doc. Nr.:
	Utgåva/datum: 3/210826	Ersätter: 2/181218	Sida: 2/5
Dokumentnamn: <p style="text-align: center;">INTEGRITETSSKYDDSPOLICY</p>			

Kvalitet, Säkerhet & Miljö

medvetenhet, och utbildning. Det är varje chefs ansvar att tillse att all personal som hanterar personuppgifter har tillräcklig kunskap och tekniska resurser för att förhindra intrång i registrerades integritet.

Personuppgiftsbehandlingen ska vara laglig

Personuppgiftsbehandling är endast tillåtet om individ samtyckt till behandlingen eller om annan rättslig grund styrker behandlingen.

De rättsliga grunderna NordArom AB kan tillämpa är:

- Intresseavvägning, t.ex. insamling och lagring av prospektuppgifter.
- Fullgörande av avtal, t.ex. vid ett anställningsavtal.
- Fullgörande av rättsligförpliktelse, t.ex. faktureringsunderlag för bokföringsskyldigheten.
- Samtycke

Information om personuppgiftsbehandlingen ska alltid ges

Då personuppgifter systematiskt samlas in (offerterbjudande, ordererkännande, arbetsansökan och anställning) ska information om personuppgiftsbehandlingen ges.

Alla anställda har i sin e-postsignatur en hänvisning till <http://nordarom.se/vart-ansvar> där vi lagt upp vår externa integritetsskyddspolicy som beskriver hur NordArom hanterar personuppgifter och säkerställer att den personliga integriteten är skyddad.

Vid spontanansökningar och rekrytering skickar vi ut en informationstext gällande personuppgiftsbehandlingen och kräver in samtycke om vi anser att ansökningarna är värda att sparas. Om inte så raderas information så snart som möjligt och om det gäller en rekrytering så raderas informationen så fort processen är färdig.


Vid anställning får alla anställda skriva under ett avtal *Bilaga GDPR till anställningsavtal*. Avtalet beskriver hur NordArom behandlar den anställdes personuppgifter och även vilka rättigheter den anställde har.

Registrering av personuppgifter

NordAroms medarbetare får endast registrera relevant information om individer, alltså endast information som behövs för att utföra sina arbetsuppgifter på ett korrekt sätt. Det innebär att ingen olämplig information får registreras om den registrerade. Ett exempel är att det är relevant att registrera kundkontakts telefonnummer men inte att dennes favoritmat är pizza.

Utgångspunkten är att medarbetare inte ska registrera känsliga personuppgifter med vissa undantag, så som i vissa fall måste vi dokumentera hälsouppgifter om anställda för att bedöma arbetskapacitet eller för att förebygga ohälsa.

Känsliga personuppgifter:

	Författare/Issuer: Karin Liljebladh	Kontrollerad av/Controlled by: Johan Eriksson	Dok. nr./doc. Nr.:
	Utgåva/datum: 3/210826	Ersätter: 2/181218	Sida: 3/5
Dokumentnamn: <p style="text-align: center;">INTEGRITETSSKYDDSPOLICY</p>			

Kvalitet, Säkerhet & Miljö

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter och
- biometriska uppgifter som entydigt identifierar en person
- Brott

Var också försiktig med andra extra skyddsvärda personuppgifter så som personnummer. Personnummer ska endast registreras i de fall vi behöver dem, t.ex. för säker identifiering.

Lagring av personuppgifter

Medarbetare skall endast lagra personuppgifter på avsedda platser så som i system, digitala verktyg och pärmar. Lagringsplats samt lagringstider för respektive personuppgift finns beskrivet i *Registerförteckningen* som finns under *GDPR* i *Verksamhetssystemet*.

Registerförteckningen ska alltid hållas aktuell och uppdaterad, se avsnittet **Personuppgift ska ha en ägare** nedan för att se vilka som ansvarar för detta.

Personuppgifter ska skyddas med tillräcklig säkerhet

I den mån det är möjligt skall personuppgifter skyddas genom tekniska åtgärder och organisatoriska säkerhetsåtgärder. För att förhindra obehörig åtkomst använder NordArom inte system med otillräcklig säkerhet. NordAroms medarbetare skall alltid vara uppmärksam och hålla koll på telefon, dator, och andra verktyg som innehåller personuppgifter så att ingen obehörig får tillgång. NordAroms medarbetare skall alltid vara uppmärksam mot dataintrång och förhindra att detta sker vilket innebär att alla ska följa NordAroms *IT-policy*, se *Verksamhetssystemet/GDPR*. NordArom ska arbeta mot och säkerställa att dataintrång och andra personuppgiftsincidenter identifierats.


Det är strängt förbjudet att dela personuppgifter till obehörig, både inom och utanför NordArom.

Personuppgifter ska gallras

Personuppgifter som behandlas av NordArom AB ska ha tydliga gallringsrutiner och ska efterlevas. När dessa personuppgifter ska gallras bort finns specificerat i *Registerförteckningen*, se *Verksamhetssystemet/GDPR*.

Personuppgiftsincidenter skall anmälas

Om en personuppgiftsincident inträffar skall medarbetare agera enligt *RU.7100 Personuppgiftsincidenthantering*.

	Författare/Issuer: Karin Liljebladh	Kontrollerad av/Controlled by: Johan Eriksson	Dok. nr./doc. Nr.:
	Utgåva/datum: 3/210826	Ersätter: 2/181218	Sida: 4/5
Dokumentnamn: <p style="text-align: center;">INTEGRITETSSKYDDSPOLICY</p>			

Kvalitet, Säkerhet & Miljö

Den registrerade har rätt att utöva sina rättigheter

Den registrerade har rätt att:

- Få insyn (få information om personuppgiftsbehandlingen och vilka uppgifter som förekommer)
- Få sina uppgifter rättade
- Få sina uppgifter raderade
- Invända mot behandlingen
- Återkalla sitt samtycke

NordAroms medarbetare måste i de fall den registrerade vill utöva sina rättigheter bistå denne med detta. Rutiner för detta finner ni i *RU.7101 Efterlevnad registrerades rättigheter + blanketterna BL.7300 Begäran om registerutdrag enligt GDPR (anställd)* och *BL.7301 Begäran om registerutdrag enligt GDPR (ej anställd)*.

GDPR-krav på underleverantörer

Alla underleverantörer till NordArom som behandlar personuppgifter för NordAroms räkning skall teckna personuppgiftsbiträdesavtal med NordArom, där underleverantören försäkrar att de behandlar personuppgifterna enligt dataskyddsförordningen och NordAroms krav.

Utveckling och dataskydd

All systemutveckling, tjänsteutveckling och affärsutveckling ska ske med respekt för den personliga integriteten och beakta GDPR. All utveckling som påverkar behandling av personuppgifter ska rådfrågas DSO:n.

Personuppgiftsbehandlingar ska ha en ägare


Varje personuppgiftsbehandling ska ha en ägare, ägarens uppgift är att säkerställa att behandlingen utförs på ett korrekt sätt och att i de fall behandlingen ändras uppdatera registerförteckningen.

Ägare för personuppgiftsbehandlingar är enligt nedan:

Område	Ägare
Försäljning	Maria Spång
Produktutveckling	Karin Anderö
Inköp/Produktion	Helena Pantzar
Ekonomi och HR	Lukas Aldén
Kvalitetschef	Sarah Redeborn

Strategi för efterlevnad

Strategier och rutiner har tagits fram för att kontinuerligt säkerställa att NordArom efterlever GDPR, se *RU.7102 Strategi för efterlevnad GDPR*.

	Författare/Issuer: Karin Liljebladh	Kontrollerad av/Controlled by: Johan Eriksson	Dok. nr./doc. Nr.:
	Utgåva/datum: 3/210826	Ersätter: 2/181218	Sida: 5/5
Dokumentnamn: <p style="text-align: center;">INTEGRITETSSKYDDSPOLICY</p>			

Kvalitet, Säkerhet & Miljö

Kontakt

Frågor gällande denna policy ställs till DSO, Lukas Aldén.

Disciplinära åtgärder

En medarbetare som bryter mot reglerna i policy kan komma att bli föremål för disciplinära beslut. Inför sådana beslut skall arbetsgivaren göra en noggrann utredning.