Namn	Utgåva	Ersätter	Org. plats	Sida # (av #)
Riktlinjer för dataskydd	1.2	1.1	N/A	1(7)

Ägare	Ändrad av	Senast ändrad	Dokument typ
General Counsel	Amelia Wallace	2024-03-12	Riktlinje

Fastställd av	Fastställd datum	Status	Ersatt av
CEO	2024-04-10	Fastställd	N/A

Riktlinjer för skydd av personuppgifter

Bakgrund

Vad omfattar den här riktlinjen?

Denna Riktlinje kompletterar Hemnets *Policy för information och data,* vilken uttrycker de intentioner och regler som gäller för användande och skydd av information, informationssystem och data (inklusive personuppgifter) på Hemnet. I Policyn anges att vi ska bedriva vår verksamhet på ett sätt som säkerställer att vi skyddar och hanterar vår data inklusive personuppgifter i enlighet med tillämplig dataskyddslagstiftning (varvid avses Dataskyddsförordningen och svensk lag som kompletterar Dataskyddsförordningen) och våra intressenters skäliga förväntningar. Detta dokument utgör Hemnets riktlinjer för skydd av personuppgifter och beskriver vad Hemnet ska göra för att åstadkomma detta.

Detaljerade instruktioner och rutiner kan komplettera denna Riktlinje där så är lämpligt.

Publicering på hemnet.se och därtill hörande personuppgiftsbehandling faller under Hemnets utgivningsbevis och omfattas inte av dessa riktlinjer i sin helhet (se nedan under “Utgivningsbevis”).

Vem bör läsa denna riktlinje?

Samtliga anställda och konsulter på Hemnet.

Varför har vi skapat den här riktlinjen?

För att förtydliga vad vi på Hemnet behöver göra för att nå de mål som är uppsatta med avseende på skydd av personuppgifter i *Policy för information och data*.

Information

Övergripande struktur för styrning

Hemnet ska ha ett strukturerat arbetssätt för regelefterlevnad varvid Hemnets Legal har det övergripande ansvaret och ska säkerställa att Hemnet på ett rimligt sätt kan styrka efterlevnad enligt principerna om ansvarsskyldighet i GDPR. De operativa inslagen av arbetet med personuppgiftsskydd hanteras i enlighet med vid var tid gällande Target Operating Model för dataskydd varvid framför allt Legal, Infosec Officer, systemägare och chefer har viktiga roller. Denna ägs av Legal och uppdateras löpande för att säkerställa att åtgärder och resurser vid var tid är adekvata.

Hemnet ska eftersträva att skydd av personuppgifter är en integrerad del av verksamheten och en naturlig del av vår affärskultur.

Några nyckelbegrepp inom skydd av personuppgifter

Vad är en personuppgift?
Alla uppgifter som direkt eller indirekt (tillsammans med annan uppgift) kan identifiera en nu levande person anses vara personuppgifter. Definitionen är bred och mycket av det som vid en första anblick kanske inte verkar vara en personuppgift kan alltså vara det, och då omfattas behandlingen av dataskyddslagstiftningen.

Vad menas med behandling av personuppgifter?
Varje form av hantering av personuppgifter kallas inom dataskyddslagstiftningen för "behandling": insamling, överföring, delning, analys, lagring, upp-backning, förädling o.s.v. En behandling kan vara att man samlar in uppgifter via ett Google formulär och sedan sparar ett Google Sheet med en namnlista med e-postadresser, eller att du senare använder listan som underlag för att skicka ut mail. Även helt passiv lagring av personuppgifter är "personuppgiftsbehandling".

Vem är personuppgiftsansvarig?
När vi samlar in och behandlar personuppgifter för vår egen räkning och för våra egna syften är Hemnet som bolag "personuppgiftsansvarig". Med den rollen följer ett stort antal skyldigheter under dataskyddslagstiftningen som syftar till att skydda de personer vars personuppgifter vi behandlar från att få sin personliga integritet kränkt.

Vad är ett personuppgiftsbiträde?
Den som behandlar personuppgifter utan att ha ett eget syfte med behandlingen utan enbart följer den personuppgiftsansvariges instruktioner, kallas inom dataskyddslagstiftningen för "personuppgiftsbiträde". I Hemnets kontext är dem flesta leverantörer personuppgiftsbiträden.

Vad avses med ansvarsskyldighet?
Under dataskyddslagstiftningen är vi skyldiga att kunna visa på att vi möter alla lagkrav. Det ställer i sin tur krav på att vi inte bara göra rätt, utan också på att vi behöver kunna visa t.ex. genom dokumentation, avtal och systemlogik, att vi efterlever lagen.

Laglighet och grundläggande principer

Säkerställande av laglighet

Principerna som anges här nedan är stommen i allt arbete med skydd av personuppgifter. All behandling av personuppgifter ska utvärderas mot de grundläggande principerna som anges nedan. Verksamheten ska få relevant stöd för att göra sådana bedömningar, och kan alltid vända sig till Legal för råd.

Grundläggande principer för laglig behandling
På Hemnet ska vi beakta följande principer för personuppgiftsbehandling:

- Ändamålsbegränsning - *Personuppgifter får endast behandlas för specifika, explicita och legitima ändamål.*
- Laglighet, Korrekthet och Transparens - *Behandling måste ha laglig grund (se nedan) och vara rättvis och transparent i relation till de individer som berörs. Personuppgifter som vi behandlar*

ska vara korrekta och om nödvändigt uppdaterade. I den mån personuppgifterna är felaktiga i förhållande till de ändamål för vilka de behandlas ska raderas eller rättas utan dröjsmål.

- Lagringsminimering - *Personuppgifter ska inte sparas längre än nödvändigt med hänsyn till ändamålet.*
- Uppgiftsminimering - *Personuppgifter ska vara adekvata, relevanta och begränsade till vad som är nödvändigt med hänsyn till ändamålet.*
- Integritet och Konfidentialitet - *Personuppgifter ska behandlas på ett sätt som säkerställer skyddet av personuppgifter, med användning av lämpliga tekniska eller organisatoriska åtgärder.*

Laglig grund

För att behandling av personuppgifter ska vara förenlig med dataskyddslagstiftningen måste varje behandling ha en laglig grund. Det finns flera olika lagliga grunder. Dessa framgår av dataskyddslagstiftningen. För Hemnet är det framförallt följande fyra lagliga grunder som vi kan använda oss av:

Intresseavvägning

Detta är den vanligaste typen av skäl till att vi behandlar personuppgifter: vårt legitima intresse av personuppgiftsbehandlingen väger tyngre än de risker som det kan innebära från ett integritetsperspektiv, för de individer det berör. Att använda intresseavvägning som laglig grund förutsätter också att vi känner oss trygga med att behandlingen i fråga ligger inom ramen för de skäliga förväntningar som berörda individer har. I det här fallet ber vi inte om godkännande inför, men möjliggör däremot för en person att tacka nej (“opt-out”) i de fall personen har rätt under tillämplig dataskyddslagstiftning att invända mot sådan behandling.
Det kan t.ex. handla om att vi sparar uppgifter om kunder i ett CRM system eller skickar ut en användarundersökning till de som valt att använda någon funktion på Hemnet.se.

Rättslig förpliktelse

Om vi behöver behandla personuppgifter för att kunna möta skyldigheter i annan lagstiftning, så kan vi göra det med hänvisning till att det är nödvändigt för fullgörande av rättslig förpliktelse.
Ett exempel är Bokföringslagen som ställer krav på att vissa underlag behöver arkiveras och sparas under en period om sju år.

Fullgörande av avtal

Behandling som är nödvändig för att kunna fullgöra skyldigheter under ett avtal kan normalt stödjas på denna lagliga grund (“fullgörande av avtal”). Ett anställningsavtal är ett exempel på ett sådant avtal. Hemnet kommer att behandla ett antal personuppgifter om sina anställda för att kunna uppfylla sin del av avtalet som t .ex. att betala ut lön.

Samtycke

Samtycke som laglig grund ska användas begränsat och endast i den mån vi inte ser att intresseavvägning kan användas. Samtycke ska heller inte användas när det föreligger en beroendeställning mellan den registrerade och den personuppgiftsansvariga, vilket är vanligt till exempel i relation till anställda. Ett samtycke ska vara baserat på korrekt, tydlig och komplett information; bland annat vilka personuppgifter som samlas in och för vilka syften. Ett samtycke kan närsomhelst återkallas, och då måste vi upphöra med behandlingen.

Transparens
Hemnet ska säkerställa att personuppgiftsbehandling är transparent mot de olika grupper av individer som berörs av den: medarbetare och kandidater, besökare i Hemnets kanaler, mäklare och privatkunder. För varje sådan grupp individer ska det finnas relevant och lättillgänglig information om Hemnets behandling. Sådan information kan presenteras i form av personuppgifts-policies eller liknande dokument och ska möta kraven i dataskyddslagstiftningen.

Känsliga personuppgifter
Känsliga personuppgifter (såsom begreppet definieras i tillämplig dataskyddslagstiftning) ska bara behandlas efter särskilt noga övervägande och med säkerställande av att uttryckligt samtycke eller annan tillämplig laglig grund finns för sådan behandling.

Undantag från dataskyddslagstiftningen inom ramen för publicering på Hemnet.se
Hemnet har ett utgivningsbevis vilket betyder att publicerad information i Hemnets kanaler omfattas av samma grundlagsskydd för yttrandefriheten som radio, TV och tidningar har. Detta betyder bland annat att dataskyddslagstiftningen, i stora delar, inte är tillämplig på personuppgiftsbehandling i samband med publicering i Hemnets kanaler där yttrandefrihetsgrundlagen istället är tillämplig. Kraven på relevanta säkerhetsåtgärder och rapportering i vissa fall av personuppgiftsincidenter gäller dock även för dessa delar av verksamheten. Personuppgiftsbehandling som följer på insamling av data via cookies och liknande teknologier i hemnets kanaler omfattas som utgångspunkt inte av undantaget.

Behandlingsregister (Förteckning över personuppgiftsbehandling)
Hemnet ska ha ett vid var tid uppdaterat behandlingsregister över den personuppgiftsbehandling som sker i verksamheten och som faller under dataskyddslagstiftningen. Registret ska även innehålla principer för gallring och uppgift om laglig grund. Det ska finnas relevanta rutiner för att säkerställa att behandlingsregistret hålls uppdaterat.

Rättigheter för de registrerade
Den som blir föremål för behandling av personuppgifter (kallas i dataskyddslagstiftningen för den “registrerade”) har ett antal rättigheter som vi är skyldiga att respektera. Det ska finnas relevanta rutiner för att säkerställa att frågor som rör utövande av rättigheter behandlas korrekt av medarbetare med relevant kunskap och att vår support har tydliga rutiner för vem de kontaktar när frågor av detta slag kommer in. De rättigheter som framförallt är relevanta för Hemnets verksamhet är följande:

- Rätt till information och tillgång
- Rätt till rättelse
- Rätt till radering

Rätt till information och tillgång handlar om att man ska få information om behandlingen i enlighet med dataskyddslagstiftningen och att man ska kunna vända sig till oss på Hemnet och få veta vilka uppgifter vi behandlar om vederbörande. Detta gäller både användare av vår tjänst och dig som anställd gentemot Hemnet som arbetsgivare. Rätten till information gäller även att den registrerade vid insamlingen av uppgifterna ska upplysas om vilka uppgifter som samlas in, syftet med behandlingen samt hur länge vi kommer att spara dem. (Se ovan under Transparens)

Rätten till rättelse innebär att man som individ kan begära att en personuppgiftsansvarig justerar eventuella felaktiga personuppgifter om en.

Under vissa begränsade omständigheter finns även en rätt att "bli glömd". Detta är inte en absolut rättighet utan det krävs en bedömning från fall till fall. Frågor som rör rätten att bli glömd ska normalt eskaleras till Legal.

Privacy by design

Varje gång vi bygger någon ny funktion, köper eller utvecklar en tjänst eller ett system av något slag ska vi alltid säkerställa att vi kan möta våra skyldigheter i dataskyddslagstiftningen såsom de presenteras i dessa riktlinjer. Vi ska tänka på att skydda personuppgifterna från att spridas, förvanskas eller förloras men vi ska också säkerställa att vi kan möta våra andra skyldigheter och att vi beaktar de grundläggande principerna (se ovan under "*Grundläggande principer för laglig behandling*").

Det kan handla om att se till att uppgifter lagras krypterat, att uppgifter anonymiseras eller pseudonymiseras eller andra tekniska lösningar för att garantera personuppgifternas integritet. Skyddet av personuppgifter ska alltså alltid vara en del i vår kravspecifikation och design och inte bli något som vi försöker lösa i efterhand. Kort och gott – vi ska tänka efter före.

Leverantörers behandling av personuppgifter

Utvärdering inför ingående av nytt leverantörsavtal
Inför ingående av nytt avtal med leverantör ska det säkerställas att:

- nya leverantörer analyseras från integritetsperspektiv - d.v.s. att det identifieras om leverantören behandlar personuppgifter för Hemnets räkning och - om ja - att leverantörens förmåga att efterleva Dataskyddslagstiftningen utvärderas, samt att
- formkrav som uppställs i Dataskyddslagstiftningen efterlevs med avseende på avtalsinnehåll i personuppgiftsbiträdesavtal (se nedan under *Biträdesavtal och överföring till tredje land*).

Legal ska tillse att verksamheten får relevant stöd i detta arbete. Inför förlängning av leverantörsavtal och annars där så är motiverat, ska leverantörers efterlevnad av biträdesavtal och förmåga att efterleva Dataskyddslagstiftningen följas upp på lämpligt sätt. Vid personuppgiftsincidenter som inträffar hos leverantörer ska leverantörens förmåga till relevanta säkerhetsåtgärder utvärderas på nytt.

Biträdesavtal och överföring till tredje land

Så fort vi ber någon att utföra en behandling av personuppgifter som vi är personuppgiftsansvariga för måste vi säkerställa att behandlingen sker med de krav och begränsningar som vi satt upp, och i enlighet med dataskyddslagstiftningens krav på avtal mellan personuppgiftsansvarig och personuppgiftsbiträde. Detta ska regleras genom ett biträdesavtal, eller som det ofta benämns "DPA" eller "Data Processing Agreement".

Vi ska genom aktiva val eftersträva att personuppgifter i största möjliga månbehandlas inom EU/EES. I vissa fall behöver vi dock använda system eller köpa tjänster där leverantören behandlar personuppgifter utanför EU/EES (primärt i USA) för vår räkning, såsom personuppgiftsbiträde. Dessutom behöver vi, oavsett var personuppgifterna är lokaliserade men där leverantören själv är ett amerikanskt bolag (eller där bolag inom leverantörens koncern faktiskt eller lagligen har rätt till tillgång till personuppgifterna som leverantören behandlar för vår räkning), förhålla oss till de möjligheter som finns i amerikansk rätt för olika myndigheter att begära ut personuppgifterna. Motsvarande bedömning kan komma att behöva göras även till andra utomeuropeiska leverantörer. Före överföring av personuppgifter till leverantören sker ska vi göra en bedömning avseende

lagligheten av överföringen, i varje enskilt fall, med utgångspunkt i vid var tid tillgänglig dataskyddsvägledning. Inom ramen för bedömningen utvärderas vilka särskilda åtgärder som behöver vidtas för att säkerställa att personuppgifterna får en adekvat skyddsnivå. Exempel på skyddsåtgärder är att säkerställa att EU-kommissionen har beslutat att landet i fråga har en adekvat skyddsnivå för personuppgifter, om leverantören är certifierad under ett ramverk som EU-kommissionen anser ha en adekvat skyddsnivå (t.ex. EU-US Data Privacy Framework) eller att vi ingår så kallade standardavtalsklausuler (även kallat Standard Contractual Clauses, "SCC"), framtagna av EU-kommissionen, med leverantören. Fråga om tredjelandsöverföring ska regleras i anslutning till biträdesavtalet och Legal ska alltid vara involverade i bedömningen.

Personuppgiftsincidenter

Hur väl vi än jobbat med "privacy by design" och riskmitigering i vår behandling av personuppgifter kan det hända att vi drabbas av personuppgiftsincidenter, d.v.s. en incident som påverkar personuppgifters konfidentialitet, integritet eller tillgänglighet. En sådan incident innebär att

- personuppgifter har blivit åtkomliga för andra än de som är behöriga (*konfidentialitet*),
- personuppgifter har förvanskats, eller ändrats på sätt som gör att de inte längre är korrekta (*integritet*), eller
- tillgången till personuppgifter är tillfälligt eller permanent påverkad. Vi kan t.ex. ha raderat dem innan det var dags för gallring, tappat bort kryptonyckeln till krypterade uppgifter etc. (*tillgänglighet*).

Beroende på sannolikheten för att en personuppgiftsincident innebär risker för de individer som berörs av den samt allvarlighetsgraden i sådana risker, kan det finnas en plikt att anmäla incidenten till Integritetsskyddsmyndigheten ("**IMY**") och/eller att informera de berörda individerna.
Alla personuppgiftsincidenter ska dokumenteras, och risken för de individer som berörs av den ska uppskattas av Legal enligt *Rutin för hantering och rapportering av personuppgiftsincidenter*. Legal bedömer även om en personuppgiftsincident är anmälningspliktig eller inte.

Riskbaserat angreppssätt - relevanta säkerhetsåtgärder

Personuppgifter ska skyddas med relevanta säkerhetsåtgärder, i förhållande till den risk en personuppgiftsincicdent skulle innebära för de individer som berörs. Hemnets arbetet med informationssäkerhet beskrivs i *Policy för Information och Data* samt underliggande styrdokument inom informationssäkerhet.

Konsekvensbedömningar (DPIA)

Inför ny personuppgiftsbehandling som kan innebära hög risk från ett integritetsperspektiv, ska en så kallad konsekvensanalys (DPIA eller Data Protection Impact Assessment) göras. En uppskattning av risken ska därför alltid göras innan en ny personuppgiftsbehandling initieras för att säkerställa att riskerna är mitigerade i tillräcklig mån. Legal ansvarar för att konsekvensbedömningar genomförs i de fall potentiellt hög risk identifierats.

Gallring

Gallringsrutiner ska implementeras i enlighet med de lagringstider som framgår av Hemnets förteckning över personuppgiftsbehandlingar för att säkerställa att principen om lagringsminimering upprätthålls.
Legal ansvarar för att gallringsrutiner implementeras och upprätthålls, med stöd av systemägare i respektive system eller chefer.

Dataskyddsombud (DPO)

Dataskyddslagstiftningen ställer om vissa kriterier är uppfyllda upp krav på att en verksamhet ska utse ett så kallat “Dataskyddsombud” som ska övervaka och stödja efterlevnad av GDPR (Dataskyddsförordningen). DPO-rollen är reglerad i lag och förutsätter registrering hos IMY. Hemnet har gjort bedömningen att verksamheten inte omfattas av kravet, och har därför inte utsett ett dataskyddsombud. Legal är ansvarig för att årligen göra en förnyad bedömning.

Rapporteringskanaler för brister i efterlevnad

Av Hemnets uppförandekod framgår vilka rapporteringskanaler som ska användas av medarbetare som upptäcker brister i efterlevnad av styrdokument. Varje medarbetare uppmanas att i första hand där möjligt ta upp frågan med den person som ärendet berör. Om det inte är lämpligt eller möjligt, kontaktas ansvarig chef. Om det inte heller är lämpligt eller möjligt uppmanas medarbetaren att kontakta sin chefs chef, Hemnets Chief People & Culture Officer eller Hemnets chefsjurist. Vidare finns möjlighet till anonym rapportering för allvarliga oegentligheter genom Bolagets visselblåsarfunktion som nås via https://report.whistleb.com/sv/hemnet.

Överträdelse av dessa riktlinjer

Överträdelser av dessa riktlinjer kommer alltid att tas på största allvar och kan leda till disciplinära åtgärder, inklusive uppsägning. Därutöver kan brott mot relevanta lagar innebära att du (och/eller Bolaget) blir föremål för rättsliga påföljder.

Relaterade dokument

- Hemnets policy för information & data
- Uppförandekod
- Rutin för hantering och rapportering av personuppgiftsincidenter
- Rutin för hantering av registrerades rättigheter