Informationssäkerhets- och personuppgiftspolicy

Denna policy har fastställts av Castellum AB:s (publ) styrelse den 29 april 2026

Innehåll

1. Bakgrund

Denna informationssäkerhets- och personuppgiftspolicy anger de allmänna principerna för Castellum AB (publ):s (”**Castellum**”) rutiner för arbete med informationssäkerhet och behandling av personuppgifter. Denna policy syftar till att skydda Castellums information, system och infrastruktur, mot hot och risker som kan påverka vår verksamhet och våra intressenters förtroende. Policyn fungerar som ett stöd för organisationen och varje medarbetare ska vara informerad om hur vi arbetar med informationssäkerhet samt hur personuppgifter ska behandlas inom Castellum. Ytterligare information kring rutinerna finns i våra interna styrdokument.

Situationer som omfattas av denna policy kan exempelvis vara behandling av anställdas personuppgifter inom ramen för anställningen eller behandling av en hyresgästs personuppgifter för att kunna uppfylla våra åtaganden enligt hyresförhållandet. All personuppgiftsbehandling som sker inom Castellum eller som någon annan utför på uppdrag åt Castellum ska ske i enlighet med gällande regelverk och eventuella personuppgiftsincidenter ska hanteras skyndsamt. En hög informationssäkerhet är en viktig komponent i det sammanhanget och en incident i våra nätverks- och informationssystem kan medföra att både personuppgifter och andra informationstillgångar skadas.

Syftet med denna policy är att säkerställa en hög informationssäkerhet, dvs. konfidentialitet, integritet och tillgänglighet av information och därmed även en korrekt personuppgiftsbehandling. Eventuella brott mot denna policy kan både medföra skada för individens säkerhet och riskera att skada Castellums varumärke. Vidare kan det medföra stora ekonomiska konsekvenser med risk för sanktioner vilket skulle skada Castellums finansiella ställning och resultat.

2. Dokumentägare

Castellums informationssäkerhets- och personuppgiftspolicy ska revideras regelbundet och minst en gång per år fastställas av styrelsen. Castellums chefsjurist (Erika Taube) är dokumentägare och ansvarar för policyn.

3. Omfattning

Castellum värnar om varje individs personliga integritet och att all personuppgiftsbehandling sker i enlighet med gällande regelverk vilket är väsentligt för att upprätthålla Castellums förtroende som arbetsgivare och i förhållande till hyresgäster. En hög informationssäkerhet är väsentligt i det arbetet och generellt för att skydda informationstillgångar i våra system och nätverk.

Informationssäkerhets- och personuppgiftspolicyn är tillämplig för samtliga bolag inom Castellum-koncernen och samtliga personer som är anställda eller annars verksamma inom Castellum-koncernen eller utför uppdrag åt bolag inom Castellum-koncernen.

4. Tillämpliga regelverk

Europaparlamentets och rådets förordning (EU) 2016/679 (”**Dataskyddsförordningen**”) är direkt tillämplig i Sverige. Castellums dataskyddsarbete ska vara förenligt med Dataskyddsförordningen och uppfylla de krav som ställs för personuppgiftsbehandling och principerna för en sådan behandling.

Castellum ska därutöver följa vid var tid tillämpliga regelverk inom informationssäkerhets- och dataskyddsområdet.

5. Informationssäkerhet

5.1 Övergripande syfte

Castellums verksamhet ska vara strukturerad på ett sätt som säkerställer en hög informationssäkerhet med implementerade rutiner för att skydda nätverks- och informationssystem mot incidenter samt för att säkerställa rätt behörighet och klassning av informationstillgångar. De viktigaste principerna är:

- **Konfidentialitet**: Säkerställa att känslig information, som kunddata och finansiella rapporter, skyddas från obehörig åtkomst.
- **Integritet**: Förhindra obehöriga ändringar av information och säkerställa att data är korrekta och tillförlitliga.
- **Tillgänglighet**: Säkerställa att information och system är tillgängliga för behöriga användare när de behövs, för att stödja verksamheten.

5.2 Riskhantering

Castellum ska arbeta med informationssäkerhet enligt ett allriskperspektiv vilket innebär att arbetet ska ske strukturerat med att identifiera, analysera och minimera risker i våra system. Regelbundna riskanalyser ska genomföras för att identifiera obehörig åtkomst, minimera risk för ransomwareattacker, driftstopp och dataläckage.

5.3 Kontinuitet och krishantering

Castellum ska ha rutiner på plats för att kunna upprätthålla verksamheten vid kriser. Det inkluderar back-up, återläsning och återställning av informationstillgångar. Regelbundna återläsningstester ska genomföras samt åtgärdsplan finnas för hantering av avbrott och driftstörningar.

5.4 Nätverkssäkerhet

Castellums nätverk ska vara försedda med skyddsfunktioner för att motverka obehörig åtkomst. Vidare ska löpande arbete ske för att skydda organisationen mot skadlig kod och obehörig programvara.

5.5 Säkerhetstester

Castellum ska löpande genomföra säkerhetstester för att identifiera brister i informationssäkerheten. Testerna ska bland annat säkerställa att system är uppdaterade, att konfigurationer omhändertar publicerade sårbarheter samt att valda tekniska säkerhetsåtgärder för system och den digitala miljön är genomförda. Avvikelser ska dokumenteras och hanteras med konkreta förbättringsåtgärder.

5.6 Utbildning

Samtliga medarbetare ska årligen utbildas inom informationssäkerhet för att öka medvetenheten och minska risken för en incident. Koncernledningen ska tillsammans med IT-funktionen regelbundet utvärdera om ytterligare åtgärder behöver vidtas baserat på genomförda riskanalyser.

5.7 Hantering av informationssäkerhetsincidenter

Castellum ska ha tydliga rutiner på plats för att upptäcka och hantera incidenter. Om anställda eller andra som utför uppdrag åt Castellum misstänker att en incident har inträffat ska det omedelbart rapporteras till Castellums IT-funktion. Incidenter ska dokumenteras för att säkerställa spårbarhet och uppföljning. IT-funktionen ska rapportera allvarliga incidenter till Castellums compliancefunktion tillika koncernens chefsjurist. Omfattar incidenten personuppgifter gäller även rapporteringsskyldigheten enligt 6.10.

5.8 Systemförvaltningsorganisation och säkerhetsklassning

Castellum har implementerat rutiner för hantering av dataskydd och informationssäkerhet inom systemförvaltningen för att säkerställa att våra informationstillgångar är skyddade. Systemförvaltningen är uppdelad enligt en struktur där varje funktion har en objektägare (funktionens chef) med det övergripande ansvaret för funktionens system. Innan avtal tecknas om att implementera ett nytt system, ska det genomföras en analys av systemets funktion, teknik och säkerhet för att säkerställa att det uppfyller Castellums krav på informationssäkerhet. Om personuppgifter ska lagras i systemet, ska det även ingås ett personuppgiftsbiträdesavtal enligt punkt 6.4.

Objektägaren ska även vara informationsägare och säkerställa att funktionens samtliga informationstillgångar blir korrekt klassade enligt *Riktlinjer för IT-säkerhet*. Det innebär att informationsägaren har det övergripande ansvaret att besluta om klassificering och lämplig skyddsnivå. Inom förvaltningen är det respektive region VD som är informationsägare. Castellums medarbetare ska löpande klassificera informationstillgångarna enligt respektive informationsägarens beslut.

6. Personuppgiftsbehandling

6.1 Rättsliga principer

Innan varje personuppgiftsbehandling påbörjas måste Castellum kontrollera att följande principer följs:

a) **Laglighet, korrekthet och öppenhet** - Det ska alltid finnas en legal grund (se punkt 6.2 nedan) för personuppgiftsbehandling och den ska vara korrekt samt präglas av öppenhet.

b) **Ändamålsbegränsning** - Det ska säkerställas att ändamålen för personuppgiftsbehandlingen finns uttryckligt angivna och att dessa är lagliga samt att uppgifterna inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

c) **Uppgiftsminimering** - Personuppgifterna som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

d) **Korrekthet** - Personuppgifterna ska vara korrekta och om nödvändigt uppdaterade och alla rimliga åtgärder ska vidtas för att felaktiga uppgifter rättas eller raderas.

e) **Lagringsminimering** - Personuppgifter ska inte lagras under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

f) **Ansvarsskyldighet** - Personuppgifterna ska skyddas med lämpliga tekniska och organisatoriska åtgärder så att de inte blir åtkomliga för obehöriga, förstörs eller skadas.

6.2 Legal grund

För att få behandla personuppgifter krävs att någon av de legala grunder som specificeras i Dataskyddsförordningen föreligger. I praktiken är fyra legala grunder relevanta för Castellum, varav punkterna nedan är de som Castellum baserar sin personuppgiftsbehandling på:

(i) **Samtycke** - Om en registrerad har lämnat samtycke till behandling av sina personuppgifter utgör detta en legal grund. Samtycket ska alltid vara frivilligt och kunna återkallas. Samtycke får inte användas i situationer där det finns en obalans mellan parterna, exempelvis i relationen mellan anställd och arbetsgivare.

(ii) **Fullgörande av avtal** - Om det är nödvändigt att behandla personuppgifterna för att fullgöra ett avtal i vilket den registrerade är part, till exempel för att Castellum ska kunna uppfylla sina åtaganden enligt ett anställningsavtal och kunna betala ut lön.

(iii) **Fullgörande av rättslig förpliktelse** - Om det är nödvändigt för att fullgöra en rättslig förpliktelse, till exempel då Castellum i egenskap av arbetsgivare har en rättslig förpliktelse att lämna uppgifter om beskattning till skattemyndigheten.

(iv) **Intresseavvägning** - Om man vid en avvägning kommer fram till att behandlingen är nödvändig för ändamål som rör Castellums berättigade intresse och att dessa intressen väger tyngre än den registrerades intressen eller grundläggande rättigheter och friheter och kravet på skydd av personuppgifter.

6.3 Transparens och informationsgivning

Den registrerade ska informeras om att dennes personuppgifter kommer att behandlas, vilket eller vilka bolag som kommer utföra behandlingen och för vilket ändamål. Sådan information ska också lämnas vad avser användningen av cookies.

6.4 Personuppgiftsbiträdesavtal

Om en extern part behandlar personuppgifter på uppdrag av Castellum eller om Castellum behandlar personuppgifter på uppdrag av en extern part måste Castellum ingå ett personuppgiftsbiträdesavtal med aktuell part. Personuppgiftsbiträdesavtalet ska vara förenligt med denna policy.

6.5 Behandling av särskilda kategorier av personuppgifter

Som huvudregel är personuppgiftsbehandling som avslöjar exempelvis ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter om hälsa eller uppgifter om en fysisk persons sexuella läggning förbjuden. Castellum behandlar endast särskilda kategorier av personuppgifter om det finns ett uttryckligt stöd i Dataskyddsförordningen.

6.6 Konsekvensbedömning avseende dataskydd

Om en typ av behandling sannolikt leder till en hög risk för fysiska personers integritet måste Castellum genomföra en konsekvensbedömning innan behandlingen påbörjas. I samband med en konsekvensbedömning ska Castellums dataskyddsombud involveras (se punkt 6.9 nedan).

6.7 Internt register över personuppgiftsbehandling

Varje Castellum-bolag som agerar i egenskap av personuppgiftsansvarig, ansvarar för att följa Dataskyddsförordningen och annan tillämplig dataskyddslagstiftning och ska även kunna visa att Dataskyddsförordningen följs. Det sker genom att varje personuppgiftsansvarig ska föra ett register över samtliga behandlingar som Castellum utför inom ramen för sin verksamhet.

6.8 Den registrerades rättigheter

Dataskyddsförordningen fastställer ett antal grundläggande rättigheter som den registrerade har rätt att utöva i samband med Castellums behandling av personuppgifter. Castellum ska ha rutiner på plats för att kunna säkerställa att den registrerades rättigheter kan tillvaratas.

a) **Rätt till rättelse, radering och begränsning** - Rimliga åtgärder ska vidtas för att säkerställa att inkorrekta personuppgifter rättas, görs fullständiga eller raderas utan oskäligt dröjsmål.

b) **Rätt att göra invändningar** - Den registrerade har rätt att invända mot Castellums behandling av personuppgifter om den har baserats på intresseavvägning, se punkt 6.2(iv) ovan.

c) **Rätt till tillgång** - Den registrerade har rätt att från Castellum få en bekräftelse på om personuppgifter behandlas eller inte och, om så är fallet, få tillgång till sina personuppgifter genom att ges en kopia av de personuppgifter som behandlas.

d) **Rätt till dataportabilitet** - Castellum ska, på begäran av den registrerade, tillhandahålla de personuppgifter som behandlas och berör den registrerade.

e) **Rätt att återkalla samtycke** - Den registrerade har rätt att när som helst återkalla ett lämnat samtycke, se punkt 6.2 (i) ovan.

6.9 Dataskyddsombud

Castellum har utsett ett dataskyddsombud som ska utföra de uppgifter som anges i Dataskyddsförordningen. Det omfattar bland annat att genomföra en årlig granskning av Castellums efterlevnad av Dataskyddsförordningen, delta i konsekvensbedömningar, ha kontakt och samarbeta med tillsynsmyndigheten samt besvara frågor eller en begäran från registrerade (se punkt 6.8 ovan).

6.10 Hantering av personuppgiftsincidenter

Om anställda eller andra som utför uppdrag åt Castellum misstänker att en personuppgiftsincident har inträffat ska det omedelbart rapporteras till Castellums dataskyddsteam. Dataskyddsteamet kommer att behandla en anmälan skyndsamt och involvera de funktioner som krävs inom Castellum för att kunna bedöma innebörden av incidenten. Dataskyddsteamet kommer även att kontakta Castellums dataskyddsombud som är ansvarig för att göra en eventuell anmälan till tillsynsmyndigheten. Om det bedöms vara nödvändigt, ska en rapportering till tillsynsmyndigheten ske utan onödigt dröjsmål och inom 72 timmar efter det att Castellum har blivit medveten om incidenten.

Castellum ska dokumentera alla personuppgiftsincidenter, även sådana som inte behöver anmälas till tillsynsmyndigheten.

Information om incidenten ska i vissa fall lämnas till personen som personuppgifterna berör. Det är Castellums dataskyddsteam som gör bedömningen tillsammans med Castellums dataskyddsombud.

Castellum ska genomföra årliga utbildningar för att säkerställa att samtliga anställda är informerade om tillämpliga regelverk och Castellums rutiner kring hantering av personuppgiftsincidenter.

7. Överträdelser mot policyn

Överträdelser mot denna policy ska rapporteras till Castellums chefsjurist, vilken i sin tur meddelar styrelsen i Castellum.

Personer som är osäkra på hur Castellums informationssäkerhets- och personuppgiftspolicy ska tolkas eller hur regelverket fungerar kan kontakta Castellums IT-funktion eller dataskyddsteam för vägledning.

Bilaga 1 – Definitioner enligt Dataskyddsförordningen

Definitionerna som används i denna policy avser ha den innebörd som anges i Dataskyddsförordningen:

A. ”*Behandling*” är en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.
B. ”*Personuppgifter*” 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.
C. ”*Personuppgiftsansvarig*” är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.
D. ”*Personuppgiftsincident*” är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.