# Västra Hamnen Corporate Finance AB

Behandling av personuppgifter.

# Riktlinjer för behandling av personuppgifter

# 1 Bakgrund och syfte

## 1.1 Bakgrund

1.1.1 Lagar och regler kring hantering av personuppgifter syftar till att skydda integriteten för människor vars personuppgifter behandlas. Inom Västra Hamnen Corporate Finance AB (”Västra Hamnen Corporate Finance”) behandlas olika typer av personuppgifter, huvudsakligen i form av kontaktuppgifter kopplade till anställda eller kunder. För att säkerställa att Västra Hamnen Corporate Finance så långt det är möjligt skyddar individers integritet bedriver bolaget ett löpande arbete för skydd kopplat till behandling av personuppgifter, ett arbete som berör alla verksamma inom Västra Hamnen Corporate Finance som behandlar eller kan komma att behandla personuppgifter.

1.1.2 Västra Hamnen Corporate Finance respekterar och skyddar integriteten för sina kunder, anställda, leverantörer m.fl. Med anställda inkluderas i denna riktlinje även konsulter och andra personer som vistas i lokaler eller på områden där Västra Hamnen Corporate Finance bedriver verksamhet. Västra Hamnen Corporate Finance arbete inkluderar både tidigare och potentiellt framtida kunder och anställda. Bolaget följer gällande lagar och regler kopplade till behandling av personuppgifter och kommer att följa den nya Dataskyddsförordningen (General Data Protection Regulation, GDPR), som träder i kraft den 25 maj 2018.

## 1.2 Syfte

1.2.1 Syftet med denna riktlinje är att vidare specificera de krav som ställs på Västra Hamnen Corporate Finance, leverantörer och andra som kan komma att behandla personuppgifter på uppdrag av bolaget. Riktlinjen återspeglar Västra Hamnen Corporate Finance policy för behandling av personuppgifter samt aktuell lagstiftning och GDPR.

## 1.3 Omfattning

1.3.1 Denna riktlinje gäller för all behandling av personuppgifter oberoende av om personuppgifterna är kopplade till kunder, anställda eller andra vars personuppgifter hanteras av eller på uppdrag av Västra Hamnen Corporate Finance.

## 1.4 Risk

1.4.1 Omfattning och regler i denna riktlinje baseras på en riskanalys med fokus på den hantering av personuppgifter som sker inom Västra Hamnen Corporate Finance. Se Appendix 1 för en summering av de identifierade riskerna.

## 1.5 Rutiner

1.5.1 Den som ansvarar för rutinerna kring hantering av personuppgifter inom Västra Hamnen Corporate Finance ska säkerställa att rutiner kopplade till behandling av personuppgifter finns dokumenterade och följs upp. Huvuddrag för Västra Hamnen Corporate Finance arbete beskrivs i denna riktlinje och Appendix 1-3 och gäller för samtliga verksamheter och bolagets anställda, kunder, leverantörer och andra berörda.

### 1.6 Nivå av krav

1.6.1 De kravnivåer som återges i denna riktlinje kan vara i form av krav som är obligatoriska att uppfylla där begreppen ”måste” eller ”ska” används, eller vara krav som är starkt rekommenderade att uppfylla, där begreppet ”bör” används.

### 1.7 Definitioner

”Behandling av personuppgifter” är en åtgärd eller en 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.

”Personuppgifter” är all information som direkt eller indirekt kan identifiera en individ. Exempel på personuppgift kan vara ett namn, en e-postadress eller ett fotografi.

”Personuppgiftsansvarig” är en juridisk person som ensamt eller tillsammans med annan personuppgiftsansvarig avgör syftet med och medlen för behandlingen av personuppgifter.

”Personuppgiftsbiträde” är en juridisk person som behandlar personuppgifter på uppdrag av personuppgiftsansvarig.

”Registrerad” är individen som personuppgifterna gäller.

”Särskilda kategorier av personuppgifter” är personuppgifter innehållande uppgifter om hälsa, ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk åskådning, fackligt medlemskap eller uppgifter om sexuell läggning. Utgångspunkten är att dessa uppgifter av sin karaktär anses känsliga och därför kräver extra beaktande vid behandling och utvärdering av skydd för personuppgifter.

## 2 Riktlinjer för behandling av personuppgifter

### 2.1 Ansvar för behandling av personuppgifter

2.1.1 Västra Hamnen Corporate Finance ska säkerställa att all behandling av personuppgifter är korrekt och laglig och bolaget ska också ansvara för och kunna dokumentera att grundläggande principerna nedan efterlevs.

i) Behandling av personuppgifter måste alltid ha en angiven personuppgiftsansvarig.

ii) Västra Hamnen Corporate Finance ska tillse att aktuella lagar och denna riktlinje efterlevs för samtliga behandlingar kopplade till processer som verksamheten är ansvarig för från dess att personuppgifterna samlas in tills att personuppgifterna inte längre ska behandlas, oberoende av om behandlingen sker av bolaget eller utförs av ett personuppgiftsbiträde.

iii) All behandling av personuppgifter ska dokumenteras i Västra Hamnen Corporate Finance register över behandling av personuppgifter.

iv) Personer eller personuppgiftsbiträden som behandlar personuppgifter på uppdrag av personuppgiftsansvarig ska endast behandla personuppgifter enligt den personuppgiftsansvariges instruktioner, vilket ska regleras i avtal – se Appendix 2.

## 2.2 Grundläggande principer för behandling

2.2.1 Personuppgifter ska endast samlas in och behandlas enligt dessa principer:

i) **Laglighet, korrekthet och öppenhet:** Västra Hamnen Corporate Finance ska endast behandla personuppgifter på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade och ska se till att de personuppgifter som behandlas är korrekta och när så krävs uppdaterade

ii) **Ändamålsbegränsning:** Västra Hamnen Corporate Finance ska endast behandla personuppgifter för affärsmässiga, angivna ändamål. Innan insamlande av personuppgifter påbörjas måste Västra Hamnen Corporate Finance avgöra syftet med behandlingen och dokumentera detta i bolagets register över behandling av personuppgifter. Inför ändring av en behandling, exempelvis ett ändrat syfte, måste behandlingen föregås av en ny bedömning innan sådan ändring sker för att säkerställa att den ändrade behandlingen är tillåten enligt gällande lag och denna riktlinje.

iii) **Uppgiftsminimering:** Västra Hamnen Corporate Finance ska endast använda de personuppgifter som krävs för det aktuella syftet med behandlingen. Personuppgifterna som behandlas ska vara nödvändiga för att uppfylla syftet. Anonymiserade uppgifter ska användas så långt det är möjligt under förutsättning att det inte kräver en orimligt stor insats.

iv) **Lagringsminimering**: Västra Hamnen Corporate Finance ska inte spara personuppgifter längre tid än vad som behövs för att uppfylla det angivna ändamålet eller för att efterleva legala krav. En behandling ska ha en angiven gallringsperiod vilken definierar när personuppgifterna ska raderas eller anonymiseras. Gallringsfrekvens ska finnas angiven i bolagets register över behandling av personuppgifter.

v) **Integritet och konfidentialitet:** Västra Hamnen Corporate Finance ska implementera tekniska och organisatoriska åtgärder för att skydda personuppgifter mot oavsiktlig eller olovlig utplåning, förlust, ändring, spridning eller annan otillåten behandling.

## 2.3 Legal grund för behandling av personuppgifter

2.3.1 Behandling av personuppgifter ska alltid ske på en legal grund vilket innebär att någon av förutsättningarna angiven i gällande lag ska vara uppfyllt. Beroende på den legala grunden kan kraven på Västra Hamnen Corporate Finance variera. Samtycke är en form av legal grund som kräver att ett antal krav ska vara uppfyllda för att samtycket ska vara giltigt. Ett ogiltigt samtycke utgör ingen legal grund för en behandling och kan därmed medföra att behandlingen är olaglig.

i) En behandling ska ske baserat på en legal grund, vilken ska dokumenteras i bolagets register över behandling av personuppgifter.

ii) Om legal grund för en behandling utgörs av en intresseavvägning bör VD godkänna den legala grunden innan behandlingen sker.

iii) Om legal grund för en behandling utgörs av samtycke krävs att samtycket uppfyller följande krav:

Samtycket ska vara:

a) Tydligt och för ett angivet syfte.
b) Dokumenterat i lämplig form.
c) Lättförståeligt och enkelt att urskilja för den registrerade.
d) Vara givet genom en aktiv handling. Samtycke i form av underförstått godkännande eller förikryssade rutor är ej giltiga.
e) Möjligt för den registrerade att återkalla sitt samtycke när som helst och lika lätt som samtycket är givet. Information om rätten till återkallande ska lämnas till den registrerade innan samtycke samlas in.
f) Tydligt åtskilt från övriga villkor.
g) Givet av en registrerad som enligt lag räknas som vuxen. Samtycke kan ej lämnas av minderåriga.

iv) Automatiska beslut eller profilering av den registrerade är endast tillåtet om den registrerade har lämnat samtycke för detta, alternativt för att fullgöra ett avtal gentemot den registrerade eller att något annat undantag angivet i lag är uppfyllt.

## 2.4 Behandling av särskilda kategorier av personuppgifter och fällande domar i brottmål

2.4.1 Behandling av särskilda kategorier av personuppgifter samt fällande domar i brottmål utgör en ökad risk mot den registrerades integritet och ska endast ske om det krävs för det specifika syftet samt att något av de undantag som anges i aktuell lagstiftning är applicerbart. Behandling av dessa kategorier kräver därför ytterligare avvägning gällande risker och en konsekvensbedömning ska genomföras och bolagets VD informeras innan behandlingen påbörjas.

## 2.5 Den registrerades rätt till information

2.5.1 För att den registrerade ska kunna tillvarata sina rättigheter behöver denne få information om den behandling som sker och Västra Hamnen Corporate Finance ska därför lämna sådan information till den registrerade. Informationen ska vara tydlig och enkel för den registrerade att tillgodogöra sig.

2.5.2 Information om behandlingen ska, när så är möjligt lämnas till den registrerade när personuppgifter samlas in, oavsett om insamlingen sker av Västra Hamnen Corporate Finance eller av annan aktör på uppdrag av bolaget.

## 2.6 Den registrerades rätt till åtgärd

2.6.1 Den registrerade ska ha rätt till följande åtgärder:

i) Den registrerade ska ha rätt att få sina uppgifter rättande om uppgifterna inte är korrekta, eller uppgifter borttagna om de inte längre finns legal grund för behandling.

ii) Den registrerade ska ha rätt till dataportabilitet, dvs. rätt att få ut alla relaterade uppgifter som den registrerade har tillhandahållit Västra Hamnen Corporate Finance i ett elektroniskt format,

om behandlingen sker automatiskt och under förutsättning av samtycke från eller avtal med den registrerade.

iii) Den registrerade ska ha rätt att få prövat om den registrerade och dennes uppgifter helt ska raderas.

iv) Den registrerade ska ha rätt att avsäga sig framtida behandling av personuppgifter för marknadsföringsändamål inkluderat profilering genom en så kallad ”opt out”.

v) Den registrerade kan även ha rätt till att behandling av den registrerades personuppgifter begränsas i väntan på utredning av en behandling.

## 2.7 Begäran om åtkomst eller åtgärd

2.7.1 En förfrågan från den registrerade gällande hur den registrerades personuppgifter behandlas eller begäran om åtgärd, exempelvis rättning av uppgifter, ska inkomma skriftligen via e-post till info@vhcorp.se. Denna e-postadress är tillämplig för samtliga förfrågningar om information, även för bolagets egna anställda.

## 2.8 Överföring av personuppgifter till tredje part

2.8.1 Västra Hamnen Corporate Finance ska endast lämna över personuppgifter till tredje part under förutsättning att överföringen har legal grund samt följer de principer och krav som angivits i denna riktlinje. Innan överföring av personuppgifter sker ska Västra Hamnen Corporate Finance beakta risker kopplade till överföringen och dokumentera ansvarsförhållandet mellan parterna.

## 2.9 Överföring av personuppgifter utanför EU/EES

2.9.1 Västra Hamnen Corporate Finance ska inför en överföring av personuppgifter ta särskild hänsyn till om personuppgifterna kan komma att överföras utanför EU/EES, exempelvis vid användandet av en molntjänst där lagring sker på servrar utanför EU/EES. Bolaget ska endast föra över personuppgifter utanför EU/EES samt tillåta sådan överföring om överföringen är tillåten enligt gällande lag, överföringen sker för affärsmässigt syfte samt att Västra Hamnen Corporate Finance fått garantier om att överföring och övrig behandling av personuppgifterna som hanteras av annan aktör kommer att ske enligt gällande lag.

## 2.10 Användande av personuppgiftsbiträde

2.10.1 Västra Hamnen Corporate Finance ska endast anlita ett personuppgiftsbiträde som ger tillräckliga garantier om att personuppgiftsbiträdet genomför lämpliga tekniska och organisatoriska åtgärder för att kunna uppfylla kraven i aktuell lagstiftning samt kunna säkerställa att den registrerades rättigheter skyddas. Ett personuppgiftsbiträde kan exempelvis vara en leverantör av tjänster för outsourcing eller en webbaserad lösning, eller en extern firma som hanterar löneuppgifter på uppdrag av Västra Hamnen Corporate Finance. Om ett personuppgiftsbiträde används skall riktlinjerna i Appendix 2 tillämpas.

## 2.11 Marknadsföring

2.11.1 Vid aktiviteter kopplade till marknadsföring, inkluderat direktreklam, ska Västra Hamnen Corporate Finance säkerställa att behandling av personuppgifter sker enligt gällande lag och branschpraxis. Detta inkluderar bland annat att Västra Hamnen Corporate Finance för externa webbsidor där bolaget kan komma att samla in eller på annat sätt behandla personuppgifter ska informera besökaren om denna behandling, exempelvis gällande förekomst av cookies. För närvaro på sociala medier ska Västra Hamnen Corporate Finance säkerställa att krav på

information om den aktuella behandlingen uppfylls.

## 2.12 Utveckling av tjänster, produkter och processer

2.12.1 Skydd för personuppgifter ska inom Västra Hamnen Corporate Finance vara en naturlig del när nya tjänster, produkter eller processer utvecklas eller upphandlas. När så är möjligt ska alternativ som stärker skydd för integritet väljas och riktlinjerna i Appendix 3 skall användas.

## 2.13 Säkerhet och personuppgiftsincident – tekniska och organisatoriska åtgärder

2.13.1 Vid behandling av personuppgifter ska Västra Hamnen Corporate Finance säkerställa att tillräckliga och lämpliga åtgärder vidtagits för att skydda dessa uppgifter, inkluderat både åtgärder av teknisk och organisatorisk karaktär. Underlag för dessa åtgärder identifieras lämpligen genom en riskanalys. Bedömningen ska även ta hänsyn till affärsprocesser och berörda IT-system. Detta för att säkerställa att personuppgifter skyddas mot oavsiktlig eller otillåten radering, utplåning, ändring, spridning, otillåten åtkomst eller annan form av olaglig behandling. Säkerhet ska även vara en del i både organisatoriska projekt och teknisk utveckling.

2.13.2 IT-system vilka behandlar personuppgifter ska ha implementerat lämpliga säkerhetsåtgärder för de typer av uppgifter som behandlas.

2.13.3 Västra Hamnen Corporate Finance bör eftersträva användande av lämpliga uppförandekoder och certifieringsmekanismer utfärdade av behörig tillsynsmyndighet eller nationellt ackrediteringsorgan enligt gällande lag för att kunna påvisa efterlevnad av aktuella krav kopplade till behandling av personuppgifter.

2.13.4 Västra Hamnen Corporate Finance ska ha en dokumenterad process för att hantera personuppgiftsincidenter. En personuppgiftsincident kan innefatta exempelvis en oavsiktlig förlust av personuppgifter. Om det inte är osannolikt att incidenten medför en risk för registrerades rättigheter och friheter ska berörd myndighet informeras om en sådan incident utan onödigt dröjsmål och inom 72 timmar.

2.13.5 Västra Hamnen Corporate Finance ska ha en dokumenterad process för att vid behov informera de registrerade vid en inträffad personuppgiftsincident utan onödigt dröjsmål.

## 2.14 Konsekvensbedömning

2.14.1 Om en behandling av personuppgifter sannolikt leder till en hög risk för den registrerades integritet, rättigheter och friheter ska en konsekvensbedömning utföras innan behandlingen påbörjas. Exempel på behandlingar kopplad till hög risk är behandling av särskilda kategorier av personuppgifter eller behandlingar där ny teknik används. En konsekvensbedömning har till syfte att identifiera risker kopplade till en behandling, samt att bedöma sannolikheten och konsekvensen om riskscenariot inträffar. Detta för att riskminimerande åtgärder ska kunna vidtas.

2.14.2 Konsekvensbedömningen måste utvärderas regelbundet för att säkerställa att bedömningen är aktuell och att vidtagna åtgärder över tid medför ett lämpligt skydd. Om en behandling som tidigare genomgått en konsekvensbedömning ändras, exempelvis genom ändrad teknisk lösning, ska en ny konsekvensbedömning genomföras.

## 2.15 Internkontroll

2.15.1 För att Västra Hamnen Corporate Finance ska kunna kontrollera den behandling av

personuppgifter som sker behöver ett antal interna kontroller finnas implementerade och utföras på regelbunden basis. För att möjliggöra detta finns ett antal grundläggande kriterier för dokumentation kopplad till internkontroll:

i) Det ska finnas en process för att säkerställa att Västra Hamnen Corporate Finance har ett aktuellt register över de behandlingar som sker inkluderat syftet med behandlingen, gallringstid, i vilket system behandlingen sker, integrationer gällande hur personuppgifter flödar och typ av information som behandlas.

ii) Det ska finnas en process för genomförandet av konsekvensbedömning när ett nytt IT-system eller en lösning utvecklas eller köps in, när särskilda kategorier av personuppgifter behandlas eller annan förhöjd risk kan förväntas föreligga.

iii) Det ska finnas en kartläggning över vilka system som behandlar särskilda kategorier av personuppgifter.

## 2.16 Medvetenhet

**2.16.1** För att Västra Hamnen Corporate Finance ska kunna efterleva gällande lagar och krav kopplade till behandling av personuppgifter krävs en förståelse inom bolaget gällande hur behandling ska ske.

2.16.2 Alla anställda på Västra Hamnen Corporate Finance ska ha genomgått en grundläggande utbildning i behandling av personuppgifter och de anställda som har regelbunden kontakt med registrerade ska ha en utökad förståelse för den registrerades rättigheter och den registrerades möjligheter att utkräva dessa.

2.16.3 Anställda vilka hanterar särskilda kategorier av personuppgifter, exempelvis anställda i Ekonomi och HR som hanterar uppgifter om anställdas hälsa, ska ha kunskap om de ytterligare krav som ställs på sådan behandling.

2.16.4 För den person inom bolaget som ansvarar för hanteringen av bolagets personuppgifter krävs en djupare förståelse för den registrerades rättigheter och den registrerades möjligheter att utkräva dessa, hur bolaget hanterar personuppgiftsbiträden och överföring av personuppgifter, Privacy by Design samt Privacy by Default.

## 2.17 Sekretess

2.17.1 Anställda, konsulter och andra verksamma inom Västra Hamnen Corporate Finance ska endast behandla personuppgifter som är relevanta för deras uppdrag och aktuell arbetsuppgift. Personuppgifter ska inte behandlas för annat syfte, i synnerhet inte för privata syften. Personuppgifter ska inte heller spridas till obehöriga. Obehöriga kan i detta fall även inkludera kollegor och andra verksamma inom bolaget som inte har ett legitimt behov av personuppgiften.

2.17.2 Innan en anställd, konsult eller annan verksam inom Västra Hamnen Corporate Finance tillträder sin tjänst eller sitt uppdrag ska ansvarig chef hos bolaget säkerställa att den anställde, konsulten eller annan verksam skriftligen godkänner att följa Västra Hamnen Corporate Finance sekretessbestämmelser genom att underteckna ett sekretessavtal.

## 2.18 Avvikelse

2.18.1 Om en avvikelse gentemot vad som anges i denna riktlinje identifieras ska detta rapporteras till VD, alternativt till den om inom bolaget som ansvarar för bolagets rutiner kring hantering av personuppgifter.

### 2.19 Kontakt

2.19.1 Den som ansvarar för bolagets rutiner kring hantering av personuppgifter på Västra Hamnen Corporate Finance är kontaktperson för frågor rörande denna riktlinje.

2.19.2 Frågeställningar, förslag och förfrågningar kopplade till denna riktlinje och dess innehåll hänvisas till info@vhcorp.se.

## 3 Möjligheter och risker

3.1.1 Genom att vid all behandling av personuppgifter följa gällande lagar och regler, denna riktlinje samt verksamhetsspecifika rutiner kan Västra Hamnen Corporate Finance värderingar om Engagemang, kvalité och nyfikenhet vid rådgivning i samband med företagsaffärer realiseras. Genom att Västra Hamnen Corporate Finance tydligt tar ansvar för de personuppgifter som behandlas och löpande följer utvecklingen gällande integritetsskydd kan bolaget upprätthålla sin position på marknaden och erbjuda trygghet för kunder och anställda.

3.1.2 Om Västra Hamnen Corporate Finance inte efterlever gällande lagar och regler kopplat till behandling av personuppgifter kan detta medföra:

- Risk för varumärkesskada genom negativ publicitet och minskat förtroende från kunder och anställda
- Risk för direkt ekonomisk skada i form av vite på upp till 4 procent av den globala koncernens omsättning alternativ 20 miljoner euro om detta är högre
- Risk för ersättning till den person som har lidit materiell eller immateriell skada, tex genom minskade intäkter.