INTEGRITETSPOLICY FÖR BEHANDLING AV PERSONUPPGIFTER

1 Bakgrund och syfte

1.1 City Transporter AB, nedan Bolaget, värnar om sina anställdas, klienters och intressenters integritet och är mån om att alltid följa gällande dataskyddsregelverk. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

1.2 Bolaget har antagit denna policy för behandling av personuppgifter för att säkerställa att alla inom organisationen följer dataskyddsreglerna. Det här dokumentet avser att ge Bolagets anställda närmare insyn om hur advokatbyrån behandlar personuppgifter.

1.3 EU:s dataskyddsförordning som trädde i kraft den 25 maj 2018 medför ett förstärkt skydd för de personer vars personuppgifter behandlas och den ställer fler och hårdare krav på organisationer som behandlar personuppgifter.

1.4 Om en behandling av personuppgifter skulle strida mot bestämmelserna i dataskyddsförordningen, finns risk för intrång i den personliga integriteten för de registrerade, men även risk för skadat anseende för Bolaget. Vidare kan Bolaget bli skyldigt att utge skadestånd eller påföras en administrativ sanktionsavgift. Sådana konsekvenser ger ytterligare anledning för Bolaget och dess anställda att följa dessa riktlinjer.

2 Tillämpningsområde och omfattning

2.1 Policyn gäller för Bolagets alla anställda och vid var tid.

2.2 Bolagets styrelse och VD har internt ansvaret för att denna policy efterlevs. Det regulatoriska ansvaret bärs av ledningen för respektive personuppgiftsansvariga juridiska person. Informationen till anställda om integritetsskyddspolicyn ska även innefatta information om att överträdelse av policyn kan komma att medföra t.ex. arbetsrättsliga konsekvenser.

3 Grundläggande principer

3.1 De grundläggande principer som beskrivs nedan ska alltid iakttas när personuppgifter behandlas. Bolaget ansvarar för och är berett att visa att principerna efterlevs.

3.1.1 *Laglighet, skälighet, transparens* – Personuppgifter ska behandlas lagligt, korrekt och transparent i förhållande till den registrerade. Det innebär att varje typ av behandling ska baseras på en giltig s.k. laglig grund, såsom exempelvis fullgörande av avtal, fullgörande av en rättslig förpliktelse, utförande av en uppgift av allmänt intresse, berättigat intresse eller samtycke (se avsnitt 5 nedan). Kan man inte identifiera någon laglig grund som är tillämplig för behandlingen får behandlingen således inte utföras. Utgångspunkten för denna princip är tydlig kommunikation med den registrerade om bl.a. för vilka ändamål personuppgifterna behandlas, vilken typ av behandling som utförs, om och hur personuppgifterna delas med andra, hur länge personuppgifterna lagras och vilka som är kontaktpersoner för dataskyddsfrågor. De registrerade ska ges tydlig och transparent information om behandlingen av deras personuppgifter.

3.1.2 *Ändamålsbegränsning* – Personuppgifter får endast samlas in och på annat sätt behandlas för särskilda, uttryckligt angivna och berättigade ändamål och de får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

3.1.3 *Uppgiftsminimering* – Personuppgifter som behandlas ska vara adekvata, relevanta och inte alltför omfattande i förhållande till ändamålen. Säkerställ att uppgifterna som samlas in verkligen behövs och fråga inte efter information bara för att den kanske kan vara bra att ha.

3.1.4 *Riktighet* – Personuppgifter som behandlas ska vara korrekta och uppdaterade. Vidta löpande lämpliga åtgärder för att se till att felaktiga eller ofullständiga uppgifter rättas, exempelvis rutiner för ändring av adress vid flytt med en sammanställning av system och register där adressen lagras. Undvik att lagra kopior av uppgifterna i många system så Bolaget undviker felkällor och att information som inte är

uppdaterad sparas.

3.1.5 *Lagringsbegränsning* – Personuppgifter får inte lagras under längre tid än nödvändigt med hänsyn till ändamålen med behandlingen. När uppgifterna inte längre behövs ska dessa gallras, vilket innebär att de antingen ska raderas eller avidentifieras.

3.1.6 Principen om ansvarsskyldighet innebär att Bolaget ska kunna visa att dataskyddsförordningen efterlevs. Bolaget ska därför exempelvis dokumentera implementerade och planerade processer och åtgärder som avser dataskyddsfrågor.

Vidare ska det finnas ett register över alla typer av behandlingar av personuppgifter som utförs och Bolaget ska kunna redovisa ett sådant register för tillsynsmyndigheten när så krävs.

4 Personuppgifter

4.1 *Personuppgifter* är alla uppgifter som avser en identifierad eller identifierbar fysisk person och som direkt eller indirekt kan identifiera en person. Exempel på personuppgifter är namn, kontaktuppgifter, lokaliseringsuppgifter eller faktorer som är specifika för en persons fysiska, ekonomiska, kulturella eller sociala identitet. Uppgifter som enskilt inte når upp till kraven kan tillsammans ändå utgöra personuppgifter.

4.2 All behandling av personuppgifter omfattas av dataskyddsförordningen och dess regler. Med *behandling* menas en åtgärd eller kombination av åtgärder avseende personuppgifter som utförs helt eller delvis automatiserat. Även personuppgifter i e-post och i dokument på servrar, i en enkel lista, på webbplatser och i annat ostrukturerat material omfattas.

4.3 Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter, uppgifter om hälsa eller uppgifter om en persons sexualliv eller sexuella läggning (s.k. *särskilda kategorier av personuppgifter*) är

som huvudregel förbjuden. För att sådan behandling ska vara tillåten krävs ett giltigt undantag från förbudet. De vanligaste undantagen är att den registrerade lämnat samtycke eller själv offentliggjort uppgifterna, för att utöva rättigheter eller fullgöra skyldigheter inom arbetsrätten, för att kunna fastställa, göra gällande eller försvara rättsliga anspråk eller för hälso- och sjukvårdsändamål.

4.4 Behandling av *personnummer* får bara utföras om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

4.5 Behandling av uppgifter om *lagöverträdelser* (fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder men sannolikt inte uppgift om misstanke om brott) får endast behandlas i vissa särskilda fall. Aktualiseras sådan behandling, tala med dataskyddsansvarig.

5 Laglig grund för behandlingen av personuppgifter

5.1 En behandling av personuppgifter är endast laglig om och i den mån någon av följande grunder är tillämplig.

5.1.1 Den registrerade har lämnat sitt *samtycke* till att personuppgifterna behandlas för ett eller flera specifika ändamål. Särskilda krav finns som måste vara uppfyllda för att samtycket ska vara giltigt.

5.1.2 Behandlingen är nödvändig för att *fullgöra ett avtal* i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

5.1.3 Behandlingen är nödvändig för att *fullgöra en rättslig förpliktelse* som åvilar Bolaget. Som exempel kan här nämnas kontrolluppgifter som lämnas till Skatteverket.

5.1.4 Behandlingen är nödvändig för att skydda intressen som är av *grundläggande betydelse* för den registrerade eller för en annan fysisk person (t.ex. när det är fara för

livet).

5.1.5 Behandlingen är nödvändig för att utföra en *uppgift av allmänt intresse* (t.ex. med anledning av myndighetsutövning).

5.1.6 Behandlingen är nödvändig för ändamål som rör Bolagets eller tredje parts intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, (*intresseavvägning*). Vid intresseavvägning tillkommer särskilda krav på dokumentation avseende den bedömning som gjorts.

6 Behandling av anställdas personuppgifter inom Bolaget

6.1 Bolaget behandlar en rad olika personuppgifter inom ramen för anställningsförhållandet mellan Bolaget och anställda i syfte att kunna bedriva verksamheten och administrera anställningsrelationen. Nedan återfinns en kortare sammanställning av dessa personuppgiftsbehandlingar.

6.1.1 Bolaget behandlar personuppgifter så som personnummer, adress, telefonnummer och kontaktuppgifter till närmaste anhörig för att hantera och administrera anställdas anställning. Administrationen och hanteringen av anställningen tar sig uttryck genom bl.a. löneadministration, förmåner och andra förmånsprogram, pensionsavsättningar, frånvaroregistrering, semesterplanering, tidrapportering, tjänstbarhetsgrad, löne- och utvecklingssamtal. Även personuppgifter om eventuella bisysslor kan komma att behandlas av Bolaget.

6.1.2 Behandling av känsliga personuppgifter med anknytning till den anställde kan förekomma vid t.ex. sjukskrivning, rehabiliteringsutredningar, arbetsmiljöutredningar, administration av företagshälsovård samt uppgifter relaterade till medlemskap i fackförening.

6.1.3 Viss behandling av anställdas personuppgifter kan förekomma i samband med underhåll och övervakning av Bolagets system för IT och telefoni.

7 Säkerhetsåtgärder, behörighetsstyrning och åtkomst, radering

7.1 Personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna med användning av tekniska och organisatoriska åtgärder. Organisatoriska säkerhetsåtgärder kan innebära att behörighetskontroll används för de system som innehåller personuppgifter, loggning av åtkomst till personuppgifter eller att datorer och dylikt som innehåller personuppgifter ska förvaras så att obehörig åtkomst försvåras och inte lämnas framme. Exempel på tekniska åtgärder till stöd för informationssäkerhetsarbetet utgörs av back-up rutiner, adekvata brandväggar, lösenordskyddade trådlösa nätverk, uppdaterat virusskydd, lösenordsskydd för mobila enheter såsom mobiltelefoner och surfplattor, skydd mot obehörig intern åtkomst, lösenordskrav, kryptering vid behov, loggning av, åtkomst till och användning av IT-system m. m.

7.2 Bolaget bevarar inte personuppgifter längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Genom att upprätta och följa en gallringsrutin för respektive behandling säkerställer Bolaget ett strukturerat gallringsarbete.

Bolaget har bedömt att något dataskyddsombud inte behöver utnämnas för verksamheten. Denna bedömning grundar sig i att Bolaget, trots att behandlingen av personuppgifter utgör en oskiljaktig del av den verksamhet som bedrivs, varken bedriver sådan regelbunden och systematisk övervakning eller behandlar personuppgifter i en sådan stor omfattning som föranleder en skyldighet att utse ett dataskyddsombud. Bolaget har därför valt att avstå från möjligheten att utse ett dataskyddsombud.

8 Överföring till tredje land

8.1 För överföring av personuppgifter till länder utanför EU och EES (s.k. tredjelandsöverföring) gäller särskilda regler. Dataskyddsförordningen innebär att alla EU:s medlemsstater samt EES-länderna har ett likvärdigt skydd för personuppgifter och personlig integritet och därför kan personuppgifter föras över fritt inom det området utan begränsningar. För länder utanför det området finns däremot inte

några generella regler som ger motsvarande garantier och därför får tredjelandsöverföring endast ske under särskilda förutsättningar. Det här berör varje form av överföring av information över gränserna, t.ex. många online IT-tjänster, molnbaserade tjänster, tjänster för extern åtkomst eller globala databaser m.m. och behöver analyseras särskilt.

8.2 För Bolagets del innebär det ett särskilt krav på uppmärksamhet när personuppgifter ska överföras mellan Sverige och tredje land. De personuppgifter som skulle kunna komma i fråga för överföring till tredje land är framförallt uppgifter som hänför sig till advokatbyråns klienter. Anställdas personuppgifter berörs i normalfallet endast undantagsvis.

9 Konsekvensbedömning

9.1 Särskilda risker för fysiska personers rättigheter och friheter kan exempelvis förekomma i samband med en viss typ av behandling av uppgifter, särskilt känsliga uppgifter, behandling i särskilt stor omfattning, användning av ny teknik eller dylikt.

9.2 Om en ny eller ändrad personuppgiftsbehandling i visst avseende sannolikt kan komma att medföra hög risk för fysiska personers rättigheter och friheter ska en bedömning göras av effekterna av de påtänkta behandlingarna för skyddet av personuppgifter innan behandlingen påbörjas.

9.3 Innan sådan personuppgiftsbehandling påbörjas av anställd i Bolaget ska någon av kontaktpersonerna för dataskyddsfrågor kontaktas för utredning om en konsekvensbedömning krävs och vid behov utförs konsekvensbedömning tillsammans med den ansvarige.

10 Registerutdrag och utlämnande

10.1 Dataskyddsförordningen ger registrerade ett flertal rättigheter vad gäller behandling av personuppgifter. Det är Bolagets uppgift att uppfylla dessa rättigheter och tillse att tillräckliga processer härför finns för att tillmötesgå de

registrerade.

10.1.1 Den registrerade har rätt till *information* när personuppgifterna samlas in. Denna information ska tillhandahållas i en lättillgänglig skriftlig form med ett klart och tydligt språk. I dataskyddsförordningen föreskrivs ett antal tydliga krav som måste vara uppfyllda och kraven varierar beroende på om informationen har samlats in från den registrerade själv eller från tredje man.

10.1.2 Den registrerade har rätt att få bekräftelse på huruvida personuppgifter som tillhör denne behandlas, och i sådana fall få en kopia av personuppgifterna (*registerutdrag*). Denna rättighet gäller oberoende av den plats där personuppgifterna behandlas.

10.1.3 Om personuppgifter som behandlas är felaktiga eller ofullständiga kan den registrerade kräva *korrigering*. Om den registrerade visar att ändamålet för vilket personuppgifterna behandlas inte längre är tillåtet, nödvändigt eller rimligt under omständigheterna, ska de aktuella personuppgifterna *raderas*, om det inte finns några lagbestämmelser som anger annat.

10.1.4 Den registrerade har rätt att överföra personuppgifter som denne lämnat till Bolaget till annan personuppgiftsansvarig (rätt till *dataportabilitet*) om behandlingen stöds på de lagliga grunderna för avtal eller samtycke. Personuppgifterna tillhandahålls den registrerade i ett strukturerat, allmänt använt och maskinläsbart format. Om det är tekniskt möjligt kan den registrerade begära att uppgifterna överförs direkt till annan personuppgiftsansvarig. Rätten gäller endast för de personuppgifter som den registrerade själv har lämnat till Bolaget.

10.1.5 Den registrerade har i vissa fall rätt att kräva att Bolaget *begränsar behandlingen* av dennes personuppgifter, d.v.s. begränsar behandlingen till vissa avgränsade syften. Rätten till begränsning gäller bl.a. när den registrerade anser att uppgifterna är felaktiga och har begärt att personuppgifterna rättas. Den registrerade kan då begära att behandlingen av personuppgifterna begränsas under tiden uppgifternas korrekthet utreds. När begränsningen upphör ska den enskild informeras om detta.

10.1.6 Den registrerade har rätt att *invända mot behandling* av personuppgifter som stöds på legitimt intresse som rättslig grund. Vid en invändning ska Bolaget upphöra med behandlingen om man inte kan visa tvingande legitima grunder för behandlingen som överväger den registrerades intressen, rättigheter och friheter.

10.1.7 I vissa fall har den registrerade rätt att begära radering av sina personuppgifter (”*rätten att bli bortglömd*”). Ett exempel är när samtycke är den lagliga grunden för behandlingen och den registrerade återkallar sitt samtycke.

10.1.8 När personuppgifter behandlas för *direktmarknadsföring* har den registrerade rätt att när som helst invända mot behandling av personuppgifter om denne. Om en registrerad motsätter sig behandling av personuppgifter för direktmarknadsändamål ska behandling för sådana ändamål upphöra.

11 Personuppgiftsincidenter

11.1 En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring eller obehörig åtkomst till personuppgifter. Exempel på personuppgiftsincidenter kan vara stöld av kundregister, oavsiktligt avslöjande av löneinformation via e-post till fel mottagare, en anställd tar hem en arbetsdator som inte är krypterad som senare stjäls i ett inbrott och som leder till att information om anställda eller kunder avslöjas, personuppgifter publiceras på webben av misstag, en bärbar dator innehållande personuppgifter tappas bort eller stjäls, m.m.

11.2 Personuppgiftsincidenter kan behöva anmälas till tillsynsmyndigheten inom 72 timmar från upptäckten av incidenten om det är sannolikt att det föreligger en risk för fysiska personers rättigheter och friheter. Inträffade incidenter ska dokumenteras och man kan behöva underrätta berörda registrerade.

11.3 Vid en misstänkt personuppgiftsincident kontakta omedelbart VD eller styrelsen. Det är styrelsen som sedan avgör om tillsynsmyndigheten eller de registrerade behöver underrättas.

12 Övrigt

12.1 För definitioner avseende termer som används i den här policyn hänvisas till dataskyddsförordningen.

12.2 Denna policy ska uppdateras årligen eller vid behov.

Frågor

Vid frågor som anknyter till behandling av personuppgifter, vänligen kontakta info@citytrans.se.

Policy antagen av Bolagets styrelse den 12 november 2021.