BILAGA B – SÄKERHETSBILAGA

1. Allmän beskrivning av tekniska och organisatoriska säkerhetsåtgärder

1.1 Parterna är överens om att Personuppgiftsbiträdet ska vidta de säkerhetsåtgärder som följer i nedan tabell, vilka Parterna bedömer är lämpliga. Personuppgiftsbiträdet har rätt att från var tid till annan ensidigt uppdatera de angivna säkerhetsåtgärderna, sådan uppdatering ska inte materiellt påverka säkerheten för Omfattade Personuppgifter negativt.

Informationssäkerhet	Personuppgiftsbiträdet ska ha utsett en eller flera personer som ansvarar för att samordna och övervaka regler och förfaranden kring informationssäkerhet och dataskydd för att säkerställa konfidentialitet, tillgänglighet, riktighet och spårbarhet. Personuppgiftsbiträdet personal ska ha kunskap om informationssäkerhet och dataskydd samt de regler och rutiner som finns för de system där kunddata lagras. Personuppgiftsbiträdet personal ska ha kännedom om åtgärder för överträdelse av informationssäkerhetsregler.
Fysisk säkerhet	Fysisk åtkomst till lokaler där system med kunddata behandlas ska vara begränsad till endast behörig personal. Lämpligt skalskydd används för att skydda lokaler och system där kunddata behandlas. I samband med avveckling eller återanvändning av lagringsmedia ska information förstöras, avmagnetiseras eller överskrivas så att informationen inte kan återläsas.
Teknisk säkerhet	**Säkerhetskopiering och dataåterställning** Säkerhetskopior av kunddata ska tas regelbundet med övervakning och loggning av genomförandet därav. Offline-säkerhetskopior ska förvaras på ett säkert sätt och vara avskilt från systemet. Personuppgiftsbiträdet ska ha specifika rutiner som reglerar vem som har åtkomst till kopior av kunddata samt vem som har behörighet att genomföra återläsningen. Insatser för dataåterställning ska loggas. **Skadlig kod.** Kunddata ska skyddas mot skadlig kod genom säkerhetsuppdateringar för att undvika att skadlig kod får obehörig åtkomst till kunddata. Skyddet ska uppdateras kontinuerligt. **Data utanför Leverantörens gränser** Personuppgiftsbiträdet ska på lämpligt sätt skydda kunddata som skickas via offentliga nätverk, t.ex. genom kryptering. Personuppgiftsbiträdet ska begränsa åtkomst till kunddata i medier som lämnar Personuppgiftsbiträdet anläggningar.
Behörighetshantering	**Beviljande av åtkomst** Personuppgiftsbiträdet ska föra och uppdatera ett register över Personuppgiftsbiträdets personal som är behöriga att få åtkomst till Personuppgiftsbiträdet system som innehåller kunddata.

	Personuppgiftsbiträdet ska inaktivera behörighetsuppgifter som inte har använts under en period på minst 90 dagar. Personuppgiftsbiträdet ska tillse att digitala användaridentiteter är personliga och unika över tid. Det ska finnas en formell process för hur användaridentiteter hanteras. Personuppgiftsbiträdet ska identifiera den personal som får bevilja, ändra eller avbryta behörig åtkomst till informationssystem. **Minsta behörighet** Personuppgiftsbiträdet ska begränsa åtkomst till kunddata till endast de personer som behöver sådan åtkomst för att kunna utföra sina arbetsuppgifter. Teknisk supportpersonal ska endast ta del av kunddata vid behov. **Integritet och sekretess** Personuppgiftsbiträdet ska förhindra obehörig tillgång till kunddata genom att anvisa sin personal att logga ut från administrativa sessioner när de lämnar lokaler som Personuppgiftsbiträdet kontrollerar samt i situationer då datorer lämnas utan uppsikt. Personuppgiftsbiträdet ska lagra lösenord på ett sätt som gör dem obegripliga medan de gäller. **Autentisering** Personuppgiftsbiträdet ska för att identifiera och autentisera användare som försöker bereda sig åtkomst till system använda säkra autentiseringsmekanismer. Personuppgiftsbiträdet ska följa branschstandardrutiner för att inaktivera lösenord som har blivit korrupta eller röjda av misstag. Personuppgiftsbiträdet ska använda branschstandardrutiner för lösenordsskydd, inklusive rutiner avsedda för att upprätthålla lösenordens sekretess och integritet när de tilldelas och distribueras, och under lagring.
Incidenthantering avseende informationssäkerhet och dataskydd	**Process för incidenthantering** Personuppgiftsbiträdet ska ha dokumenterat och till sin personal ha kommunicerat ansvar, rutiner, kontaktvägar och kommunikationsplaner vid personuppgiftsincidenter som kan omfatta kunddata. Personuppgiftsbiträdets personal ska informeras om sitt ansvar att rapportera avvikelser, risker och incidenter som kan påverka kunddata, samt ska känna till på vilket sätt det ska ske. Personuppgiftsbiträdet ska i möjligaste mån spåra utlämnanden av kunddata, inklusive vilka data som har lämnats ut, till vem och vid vilken tidpunkt. Informationssäkerhetsincidenter dokumenteras och utvärderas inom tre månader för att minska sannolikheten för liknande framtida händelser.
Kontinuitetshantering	Personuppgiftsbiträdet ska ha en plan för kontinuitet samt reservrutiner för de system som hanterar kunddata. I kontinuitetsplanerna ska krav på att informationssäkerheten bibehålls på en motsvarande nivå som under normala förhållanden ingå.

* * *