

Användarvillkor för auktoriserade servicepartners gällande B2B Connect Seller Center och Webparts Dealer Client

mellan MB Sverige (Mercedes-Benz Sverige AB Dockgatan 1, 211 12 Malmö, Sverige) (nedan kallad "**MB Sverige**") och MB Sverige:s auktoriserade servicepartner (nedan kallad "**Partner**") som deltar i B2B Connect och relaterade tjänster (B2B Connect Seller Center och WebParts Dealer Client) kallas härnäst gemensamt för "**B2B Connect**".

Kunder i detta sammanhang är Business to Business-oberoende entreprenörer som utför reparations- och underhållstjänster för fordon (t.ex. enskilda tjänsteleverantörer och vagnparks kunder) (nedan även kallade "**Kunden**").

MB Sverige och Partner benämns i det följande även "**Parterna**".

Förord

B2B Connect tillhandahålls av MB Sverige. B2B Connect är ett tekniskt ekosystem som integrerar försäljning av Mercedes-Benz originaldelar via B2B Connect Seller Center med de redan existerande onlineverktygen som finns i Mercedes-Benz Aftersales ekosystem samt reparations- och underhållslösningar, i den mån sådana är tillgängliga på den relevanta marknaden så att ett enda B2B-ekosystem formas för Kunden. För Partners erbjuds tjänster i B2B Connect genom WebParts Dealer Client och B2B Connect Seller Center. Funktioner från WebParts Dealer Client kommer därefter att migreras till B2B Connect Seller Center.

Kunden får tillgång till B2B Connect genom självregistrering och kan anpassa sina data, men onlinebeställning av Mercedes-Benz Originaldelar via B2B Connect är endast tillgänglig för Kunden efter godkännande och aktivering av Partnern i WebParts Dealer Client (även efter migrering till B2B Connect Seller Center).

Syftet med den nuvarande WebParts Dealer Client och B2B Connect Seller Center är att ge Partnern en kundorienterad och systemisk lösning online, som ett marknadsföringsverktyg inom After Sales (over the-counter försäljning) samt bidra till ökad konkurrenskraft och lönsamhet i eftermarknadsverksamheten. Bestämmelserna i det auktoriserade serviceavtalet gäller även för dessa användarvillkor.

I beställningsprocessen visas Kunddata för Partnern via WebParts Dealer Client men kommer i framtiden visas via B2B Connect Seller Center och kunna importeras till partners hanteringssystem.

§ 1 Systemkrav

För att visa Partners reservdelstillgänglighet för Kunden måste Partnern vara ansluten till Logistikbus, som tillhandahålls av MB Sverige i samarbete med MBAG. I annat fall finns det en begränsad tillgång till information.

§ 2 MB Sverige:s Tjänster, Ingående av avtal, Ändring, Deltagande och 5*Rater

MB Sverige tillhandahåller Partnern B2B Connect Seller Center och WebParts Dealer Client som möjliggör onlinebeställning av Mercedes-Benz originaldelar för Partners Kunder.

Genom MB Sverige tillhandahålls B2B Connect Seller Center och WebParts Dealer Client som gör det möjligt för Partnern att:

- se de aktiverade kunderna,
- justera listpriser,
- definiera diskonteringsräntor,
- definiera egna kundrabattkoder,
- tilldela den valda Kundrabattkoden,
- definiera egna rabattgrupper,
- definiera information om beräknad ankomsttid och support för kundförfrågningar
- få feedback om sina produkter, tjänster och övergripande prestanda från kunder via 5*Rater,

- få anpassade kampanjförslag och kampanjsupporttjänster baserat på information relaterad till transaktioner som utförs via B2B Connect med kunder (dvs. kundnamn, orderrelaterad information etc.)
- hantera orderförfrågningar och kundtransaktioner från B2B Connect och PartsLink24

När Kunder deltar i B2B Connect kan de betygsätta Partners produkter, tjänster och övergripande prestanda genom 5*Rater. Genom att delta i och använda B2B Connect Seller Center och WebParts Dealer Client bekräftar och accepterar Partnern det faktum att Kunden ger feedback och att MB Sverige kommer att få denna information i aggregerad form (som inte innehåller någon information relaterad till särskilda transaktioner) och ska ha rätt att använda denna information för marknads- och partnerprestandagranskningar och styrning av den övergripande prestandan och samarbetet med partnern. Ytterligare information om användningen av personuppgifter i detta sammanhang finns i **Bilaga 1** till dessa användarvillkor.

Utifrån de uppgifter som Kunden tillhandahåller kan Kunden beställa Mercedes-Benz originaldelar via Internet från Partnern varvid det kundspecifika priset och tillgängligheten för respektive Mercedes-Benz Originaldel visas. Förutsättningen för detta är att Kunden har registrerat sig för B2B Connect och att Partnern har aktiverat Kunden i WebParts Dealer Client. Kundens beställning skickas till Partnern via B2B Connect och kan läsas av Partnern via ett standardexportformat samt kan importeras till partners hanteringssystem.

Partnern ska vara fri att välja om och vilka av de mottagna beställningarna denne vill acceptera. Om Partnern och Kunden inte har kommit överens om något annat ska ett avtal anses ha ingåtts vid den tidpunkt då Partnern accepterar Kundens beställning genom att vidarebefordra ett ordergodkännande. Fullgörandet av avtal som görs via B2B Connect ligger inom respektive Partners eget ansvar. MB Sverige åtar sig inte heller att garantera att avtal som ingåtts eller hanteras mellan Partner och Kunden via B2B Connect fullgörs. MB Sverige har ingen som helst skyldighet att se till att de avtal som har ingåtts mellan Partner och Kund fullgörs.

MB Sverige har rätt att ändra de funktioner som tillhandahålls genom B2B Connect om en sådan ändring inte skulle kräva en ändring av dessa användarvillkor. MB Sverige ska meddela Partnern skriftligen (t.ex. e-post) minst en månad före en sådan ändring om inte annat överenskommit.

Om inget annat avtalats har MB Sverige rätt att när som helst ändra dessa användarvillkor i den utsträckning en sådan ändring är neutral för Parterna eller ensidigt fördelaktig för Partnern. I annat fall ska MB Sverige meddela Partnern skriftligen minst sex (6) veckor före en sådan ändring. Om Partnern inte invänder mot sådana ändringar skriftligen inom fyra (4) veckor efter att ha mottagit ett sådant meddelande, ska de föreslagna ändringarna bli bindande för Parterna sex (6) veckor efter meddelandet. MB Sverige ska i meddelandet underrätta Partnern om effekten av att inte invända mot sådana ändringar. Partnern har rätt att invända mot sådana ändringar. Om Partnern motsätter sig ändringen har MB Sverige rätt att säga upp Partners användning av de tjänster som berörs av ändringen.

Dessa användarvillkor ska fortsätta att gälla även för det fall att MB Sverige integrerar WebParts Dealer Client direkt i B2B Connect Seller Center med förbehåll för eventuella nödvändiga ändringar av användarvillkoren som i detta sammanhang kan implementeras i enlighet med ovanstående bestämmelser.

§ 3 Användning av B2B Connect Seller Center och WebParts Dealer Client

Partnern tar emot intresserade kunder och kan aktivera dem för onlinebeställning via WebParts Dealer Client. Aktiveringen bör ske utan onödigt dröjsmål.

Det är partners ansvar att se till att de avtalsenliga försäljningsbegränsningarna följs (i synnerhet beträffande auktoriserat serviceavtal och standarder).

Masterdata, t.ex. fastställande av rabattsatser för självdefinierade kundrabattklasser, tilldelning av Mercedes-Benz Originaldelar till självdefinierade rabattgrupper eller kampanjer etc. måste läggas in i systemet av partnern.

Partnern är fri att välja sin egen prissättning samt att bevilja och benämna kundrabatter. De priser, rabatter, rabattkoder eller kampanjer som lagras i systemet eller läggs in av Partnern visas för Kunden när denne gör beställningen. Det är Partnerns ansvar att säkerställa att uppgifterna är uppdaterade.

Partnern är skyldig att tillhandahålla sina allmänna villkor samt sina dataskyddsbestämmelser för sina kunder i WebParts Dealer Client (och att erhålla respektive godkännande i den utsträckning som krävs). Av Partnerns allmänna villkor ska det framgå tillräckligt tydligt att det är Partnern som säljer Mercedes-Benz originaldelarna. Dataskyddsbestämmelserna måste tydligt ange att Partnern är personuppgiftsansvarig för sina kunders uppgifter i samband med genomförandet av en beställning. Vidare måste Partnerns dataskyddsbestämmelser följa respektive tillämpliga dataskyddslag (inklusive eventuella informationsskyldigheter), särskilt de i den allmänna dataskyddsförordningen (GDPR). Om Partnern vid något tillfälle under giltighetstiden för dessa användarvillkor inte kan erbjuda Mercedes-Benz originaldelar i enlighet med gällande dataskyddslag, ska Partnern meddela MB Sverige härom. Partnern ska ha möjlighet att föreslå åtgärd inom en rimlig tidsperiod som krävs av MB Sverige. Om en lösning som föreslagits av Partner inte rimligen är acceptabel för MB Sverige, har MB Sverige rätt att säga upp avtalet under dessa Användarvillkor helt eller delvis med omedelbar verkan.

Syftet med B2B Connect är att online presentera Partnerns erbjudanden på Mercedes-Benz originaldelar. Kunder får endast använda B2B Connect för att ta del av dessa erbjudanden.

Användningen av B2B Connect ger inga rättigheter för Partnern till B2B Connect, URL:erna som används eller den medföljande dokumentationen (manual, guidad tur, etc.) annat än rätten till användning i enlighet med dessa användarvillkor.

Partnern åtar sig att se till att den hårdvara och programvara som används av denne vid användning av B2B Connect Seller Center och WebParts Dealer Client, i den utsträckning det är tillämpligt, inklusive arbetsstationsdatorer, surfplattor, routrar,

datakommunikationssystem och så vidare, är fria från virus, maskar, trojanska hästar etc. När det gäller data som laddas upp av Partnern åtar sig Partnern att se till att denne är innehavare av alla rättigheter till det uppladdade innehållet och fritt kan förfoga över dess användning, inklusive att sådana uppladdade data inte belastas av tredje parts rättigheter, som inte tillåter en sådan användning.

Partnern kan via B2B Connect Seller Center hjälpa kunder med att lämna klagomål riktade till MB Sverige eller med att göra andra förfrågningar som rör B2B Connect på begäran av kunden. Sådan support ska ske kostnadsfritt (ingen rätt att kräva ersättning eller ersättning för kostnader eller utgifter mot MB Sverige) och ska endast tillhandahållas på Partnerns eget ansvar och i relation till Kunden och utan att MB Sverige tar något ansvar för Partnerns användning av B2B Connect Seller Center eller ytterligare support som tillhandahålls kunderna. Detta gäller även för annan transaktionsrelaterad information som Partnern tillhandahåller åt kunder (t.ex. information om beräknad ankomsttid) i WebParts Dealer Client.

§ 4 Dataflöde

Kunden anger sina uppgifter via självregistrering på B2B Connect. Dessa data autentiseras och lagras av leverantören MB Sverige. Uppgifterna lämnas också till Partnern i B2B Connect Seller Center.

§ 5 Sekretess

Partnern ska behandla all teknisk och ekonomisk information, inklusive användningsdata från kunder, som kommer att vara direkt eller indirekt tillgänglig för dem under dessa användarvillkors giltighetstid i samband med användningen av B2B Connect med sekretess. MB Sverige gör dessa uppgifter tillgängliga för tredje part endast om det är nödvändigt för att uppfylla avtalet eller i annat fall som föreskrivs häri och om det finns ett motsvarande sekretessavtal med sådan tredje part. Uppgifter om kunder som aktiverats av Partnern eller kundens användningsdata kommer endast att användas av MB Sverige för att uppfylla avtalsförpliktelser enligt dessa användarvillkor och kommer att anonymiseras av Mercedes-Benz AG för att utveckla plattformen.

Uppgifter och handlingar som inte är klassificerade som sekretessbelagda är följande:

- allmänt känd information eller information som kommit till kännedom utan att de skyldigheter som följer av dessa Användarvillkor har överträtts,
- Information som en part bevisligen skapat eller erhållit som en del av sitt eget arbete, eller
- Information som MB Sverige bevisligen har mottagit på laglig väg från tredje part.

Part är befriad från skyldigheten att behandla information konfidentiellt om denne måste lämna ut informationen på grund av lagbestämmelser eller behöriga myndigheters beslut.

§ 6 Skydd av personuppgifter

När det gäller försäljnings- och försäljningsprocessen avseende originaldelar/tjänster via B2B Connect avser parterna att utbyta relevanta personuppgifter mellan oberoende personuppgiftsansvariga, medan MB Sverige ska vara personuppgiftsansvarig för behandlingen av personuppgifter i syfte att driva B2B Connect. Om inte annat anges har parterna i allmänhet inte för avsikt att upprätta ett gemensamt personuppgiftsansvar med avseende på deras individuella behandling av kundens personuppgifter. I den mån förhållandet mellan MB Sverige, Mercedes-Benz AG (och/eller dess dotterbolag) och/eller partner uppfyller eller kan betraktas som gemensamt personuppgiftsansvar enligt artikel 26 i GDPR, kommer parterna att ingå lämpliga avtal om gemensamt personuppgiftsansvar med respektive gemensamt personuppgiftsansvarigt i enlighet med artikel 26 i GDPR.

MB Sverige behandlar dock personuppgifter om Partner och Partners Kunder (i) på uppdrag av Partner som personuppgiftsbiträde, och (ii) vid användning av personuppgifter i 5*Rater, för support via B2B Connect Seller Center, eller för affärsanalys och Marketing Campaign Services som personuppgiftsansvarig. De bestämmelser om dataskydd som överenskommit mellan parterna framgår av **Bilaga 1** till dessa användarvillkor.

§ 7 Datakvalitet, Partnerns skyldigheter

Partnern ansvarar för att hålla den information som är nödvändig för att erbjuda/visa Mercedes-Benz originaldelar via WebParts Dealer Client (priser, rabatter, tillgänglighet, leveranstider etc.) uppdaterad.

Partnern ska regelbundet både kontrollera online och meddelanden på elektronisk väg huruvida en beställning av Mercedes-Benz originaldelar har gjorts av kunder. Partnern exporterar dessa beställningar till återförsäljarhanteringssystemet och fortsätter att behandla dem. Partnern ska behandla beställningarna inom rimlig tid och informera kunden om beställningens status. Partnern ska på ett konventionellt sätt tillhandahålla Kunden en orderbekräftelse med information om huruvida de leveranstider som kunden begärt kan hållas.

MB Sverige tillhandahåller ett lämpligt tillträdesskyddssystem och tilldelar på begäran åtkomstbehörighet till Partnern. Partnern åtar sig att se till att hans anställda använder systemet på rätt sätt, vilket inkluderar användning av lämpliga program vid åtkomst till systemet. Partnern förbinder sig att inte avslöja den åtkomstbehörighet eller informationen i åtkomstbehörigheten som tilldelats honom till någon obehörig person.

Partnern åtar sig att svara på inkommande förfrågningar om godkännande av registrering från kunder inom rimlig tid och att i samordning med MB Sverige tillhandahålla 1:a och 2:a nivåns support för WebParts Dealer Client. MB Sverige ansvarar inte för missbruk av användar-ID och lösenord som sker i Partnerns organisationsenhet eller av dennes kunder och MB Sverige fransäger sig allt ansvar för sådant missbruk.

MB Sverige förbehåller sig rätten att blockera användare vid tecken på felaktig användning och/eller missbruk. Partnern ska informeras direkt om detta.

B2B Connect är en teknisk lösning som är tillgänglig över hela världen. Partnern är ansvarig för att regelbundet kontrollera de

tillämpliga rättsliga ramvillkoren i sitt land med avseende på försäljnings- och försäljningsprocessen avseende Mercedes-Benz originaldelar på B2B Connect, medan MB Sverige förblir ansvarig för att regelbundet kontrollera de tillämpliga rättsliga ramvillkoren för driften av B2B Connect.

Partnern måste vid tillhandahållandet av de tjänster som regleras i dessa användarvillkor i synnerhet se till att alla krav i förhållande till kunderna (inklusive nödvändiga samtycken och information) efterlevs.

Under alla omständigheter gäller Mercedes-Benz Regler för Plattformen tillsammans med dessa användarvillkor som **Bilaga 2**.

§ 8 Tillgänglighet

Partnern är medveten om och accepterar att följande begränsningar, felaktigheter och störningar som är utanför MB Sverige:s kontroll kan förekomma vid tillhandahållandet och användningen av B2B Connect. Detta gäller särskilt med avseende på tillgången till internet. Störningar kan också orsakas av force majeure, inklusive strejk, lockout eller order från myndigheter, eller vara ett resultat av tekniska eller andra åtgärder (t.ex. reparationer, underhåll, programuppdateringar och förbättringar) som måste utföras på MB Sverige:s eller tjänsteleverantörers system som är nödvändiga för att säkerställa att B2B Connect tillhandahålls eller förbättras på korrekt sätt.

§ 9 Ansvar, skadeersättning

MB Sverige och Partner ansvarar var för sig för eget och sina respektive ställföreträdarens vållande av dödsfall eller kroppsskada genom uppsåt och grov vårdslöshet och ringa vårdslöshet.

MB Sverige och Partnern ansvarar vidare för ringa och strängare former av vårdslöshet enligt följande: Ansvar uppstår endast i händelse av brott mot väsentliga avtalsförpliktelser; "Väsentliga avtalsförpliktelser" är sådana där fullgörandet av skyldigheten ifråga är av väsentlig betydelse för ett korrekt genomförande av avtalet. Detta ansvar är begränsat till den typiska direkta skada som kan förutses vid den tidpunkt då avtalet ingås. I den mån skadan täcks av en försäkring som Partnern eller MB Sverige har tecknat för den aktuella skadan (exklusive totalförsäkring) ansvarar MB Sverige eller Partnern endast för eventuella nackdelar för Partnern eller MB Sverige, t.ex. högre försäkringspremier eller räntenackdelar, fram till dess att försäkringen är reglerad.

Partnern är skyldig att hålla MB Sverige skadeslös för alla skador, förluster, skulder, anspråk (inklusive krav från tredje part) och kostnader (inklusive lämpliga juridiska arvoden och kostnader) som uppstår till följd av ett klandervärt brott mot dessa villkor och de transaktioner som avses häri (inklusive men inte begränsat till partnerns användning av B2B Connect Seller Center).

§ 10 Användarvillkorens varaktighet och upphörande

Dessa användarvillkor ersätter de tidigare användarvillkoren med avseende på samma ämne med verkan från och Maj 2023 och börjar gälla vid godkännandet av dem.

Båda Parter kan säga upp avtalet under dessa användarvillkor skriftligen (skriftlighet är tillräckligt för alla uppsägningar som kan ske enligt denna § 10) med iakttagande av en uppsägningstid på tre månader till slutet av en månad. I vilket fall som helst upphör avtalet under dessa användarvillkor med uppsägningen av det auktoriserade serviceavtalet mellan parterna.

Efter att avtalet under dessa användarvillkor har upphört att gälla fortsätter bestämmelserna om dataskydd och sekretess som avses i § 4, 5 och 6 att gälla.

Vid allvarliga överträdelse av dessa Användarvillkor, såsom överföring av uppgifter som utgör brott mot tystnadsplikten enligt § 5, kan vardera Part säga upp avtalet under dessa Användarvillkor omedelbart utan iakttagande av uppsägningstid. Vid uppsägning på grund av allvarliga överträdelse av Part förbehåller sig den andra Parten rätten att kräva ersättning för ytterligare skada.

Uppsägning vid upphörande av huvudtillståndet: MB Sverige rättigheter att tillhandahålla WebParts Dealer Client och B2B Connect Seller Center till Partner härrör från ett avtal mellan MBAG och MB Sverige. MB Sverige kan säga upp avtalet under dessa användarvillkor efter skriftligt meddelande till Partnern med hänvisning till MBAG:s egna rätt att tillhandahålla WebParts Dealer Client och B2B Connect Seller Center och att dessa sagts upp eller inte förlängts av MBAG.

§ 11 Skatt

Om MB Sverige är skyldig att betala skatter och tullar som vederbörligen kan hänföras till försäljningen av produkter som publiceras på WebParts Dealer Client och B2B Connect Seller Center av Partnern eller till tjänster som publiceras på B2B Connect av Partnern och som i båda fall tillhandahålls Kunden, till exempel skatter på digitala tjänster, ska Partnern täcka alla kostnader för MB Sverige som uppstår till följd av sådana skatter och tullar. Detsamma

ska gälla för den mervärdesskatt som Partnern är skyldig att betala men som inte har betalats och som MB Sverige har hållits ansvarig för.

§12 Jurisdiktion

Avtalet under dessa användarvillkor regleras av lagen i Sverige. Den exklusiva jurisdiktionen för tvister som uppstår till följd av avtalet under dessa användarvillkor är Malmö tingsrätt om det tvistiga värdet understiger 1 000 000 kr (SEK) och Stockholms Handelskammars Skiljedomsinstitut om det tvistiga värdet överstiger 1 000 000 kr (SEK).

Bilagor till dessa användarvillkor

Bilaga 1 – Avtal om skydd av personuppgifter

Bilaga 2 – Regler för Plattformen

Bilaga 1:

Avtal om skydd av personuppgifter

B2B Connect Platform och relaterade Tjänster

mellan

[MPC/GD]

Mercedes-Benz Sverige AB

556487-1548

Dockgatan 1, 211 12 Malmö, Sverige

("MB Sverige")

och

Auktoriserad servicepartner

("ASP")

(vardera en "Part" och tillsammans "Parterna").

BAKGRUND

- (A) **MB Sverige** är ett företag i Mercedes-Benz koncernen och stöder Mercedes-Benz AG:s verksamhet i förhållande till dess återförsäljare ("återförsäljare" inklusive ISP kunder ("ISP") och auktoriserade servicepartners) i Tyskland, Europa (EU) och resten av världen ("RoW") genom att erbjuda vissa eftermarknads- och marknadsföringsrelaterade tjänster ("Tjänster", enligt definitionen nedan).
- (B) **Att** erbjuda och tillhandahålla Tjänsterna innebär överföring och behandling av Personuppgifter till och av MB Sverige för att tillhandahålla Tjänsterna till ASP:er.
- (C) **Att** europeiska och lokala dataskyddslagar föreskriver vissa krav när det gäller bland annat överföring och behandling av personuppgifter inom företagsgrupper eller distributions- eller eftermarknadsnätverk.
- (D) **Detta** avtal är avsett att ge tillräckliga garantier och skydd i samband med nationell, gränsöverskridande, EU-omfattande och världsomspännande överföring och behandling av personuppgifter enligt tillämplig dataskyddslagstiftning enligt definitionen nedan.
- (E) **Parterna ingår därför** följande avtal (nedan kallat "Avtalet").

1. DEFINITIONER

1.1 I detta avtal ska följande termer ha följande betydelser:

- (a) "Personuppgifter", "Personuppgiftsansvarig", "Personuppgiftsbiträde", "Behandling/behandling", "registrerad", "tekniska och organisatoriska åtgärder" och "tillsynsmyndighet" ska tolkas i enlighet med GDPR eller motsvarande terminologi enligt Tillämplig dataskyddslagstiftning. Underbiträde ska ha samma

betydelse som "annat personuppgiftsbiträde" i GDPR eller motsvarande terminologi enligt Tillämplig dataskyddslagstiftning.

- (b) ""Avtal" avser detta Dataskyddsavtal.
- (c) "Tillämpliga dataskyddslagar" avser GDPR, alla lokala dataskyddslagar som är tillämpliga i en medlemsstat eller annan tillämplig dataskyddslagstiftning som är tillämplig på var och en av parterna – gemensamt eller separat – vid utförande eller användning av tjänsterna. Det faktum att en Part har fullgjort detta Avtal i enlighet därmed ska inte ha till följd att någon dataskyddslag som är tillämplig på den ena Parten automatiskt ska gälla för den andra Parten/Parterna och vice versa. Säker för villkoren i detta avtal, tillämpligheten av tillämpliga dataskyddslagar för någon av parterna ska bestämmas av respektive lagar. Således, och med förbehåll för ytterligare bestämmelser och skyldigheter för parterna enligt vad som anges i detta avtal, ska varje part följa tillämpliga dataskyddslagar om och i den utsträckning som endast är tillämplig på den. Av förtydligande skäl och som exempel, när det hänvisas till de registrerades lagstadgade rättigheter enligt artikel 12-22 i GDPR eller de lagstadgade kraven för databehandling för uppdrag enligt artikel 28 i GDPR, ska sådana rättigheter eller krav endast gälla för personuppgiftsansvariga som omfattas av GDPR.
- (d) "Accepterat Land" avser ett land utanför EES som av Europeiska kommissionen anses tillhandahålla en adekvat nivå av integritetsskydd på grund av sin nationella lagstiftning eller de internationella åtaganden som landet har ingått.
- (e) "Databehandling på uppdrag av en personuppgiftsansvarig" avser behandling av personuppgifter som ska utföras på uppdrag av en personuppgiftsansvarig och ska tolkas i enlighet med artikel 28 i GDPR.
- (f) "MBAG" avser Mercedes-Benz AG, Mercedesstraße 120, 70372 Stuttgart, Tyskland.
- (g) "MB Sverige" betyder Mercedes-Benz Sverige AB, Dockgatan 1, 211 12 Malmö, Sverige
- (h) "Klausuler" avser, kollektivt, klausulerna om databehandling på uppdrag av en kontrollant och klausulerna mellan personuppgiftsansvariga.
- (i) "Klausuler om databehandling på uppdrag av en personuppgiftsansvarig" avser de bestämmelser som anges i del B.
- (j) "Klausuler om gemensamt personuppgiftsansvariga" avser de bestämmelser som anges i del A. Klausuler om gemensamt personuppgiftsansvariga ska reglera överföring och användning av personuppgifter mellan MB Sverige och ASP, varvid parterna agerar som gemensamt personuppgiftsansvariga där det föreskrivs för var och en av dem enligt tillämpliga dataskyddslagar.
- (k) "GDPR" avser Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
- (l) "Gemensamt personuppgiftsansvar" avser behandling av personuppgifter där syftet med sådan behandling bestäms gemensamt av två eller flera personuppgiftsansvariga och ska tolkas i enlighet med artikel 26 i GDPR.
- (m) medlemsstat: ett land som är medlem i EU.
- (n) "Tjänster" avser eftermarknadsrelaterade tjänster som beskrivs närmare i de relaterade separata kontrakten och delarna av detta avtal.

1.2 I detta avtal:

- a) hänvisningar till en lagbestämmelse omfattar all underordnad lagstiftning som från tid till annan utfärdas med stöd av den bestämmelsen,
- b) Hänvisningar till detta avtal inbegriper bilagor och tillägg.
- c) Rubriker skall inte beaktas vid tolkningen av detta avtal, och
- (d) om det finns någon konflikt eller inkonsekvens inom detta avtal ska konflikten eller inkonsekvensen lösas genom att klausulerna har företräde enligt inbördes ordning.

2. OMFATTNING

- 2.1 Klausulerna ska gälla mellan parterna i deras roll som personuppgiftsansvarig (eller gemensamt personuppgiftsansvarig) eller personuppgiftsbiträde i förhållande till de relevanta personuppgifter som behandlas enligt vad som närmare definieras i bilagorna till delarna A och B.
- 2.2 Eftersom parterna vill säkerställa en adekvat skyddsnivå i samband med behandlingen av personuppgifter med avseende på skyddet av de registrerades integritet och grundläggande rättigheter och friheter, ska de principer som anges i del A tillämpas på all behandling mellan personuppgiftsansvariga enligt beskrivningen däri, oavsett om det anses vara en behandling i ett gemensamt personuppgiftsansvar eller inte.
- 2.3 Varje Part, i sin egenskap av Personuppgiftsansvarig eller Personuppgiftsbiträde, ska ålägga underbiträden (om sådana finns) att tillhandahålla minst en liknande skyddsnivå och vidare säkerställa att underbiträdet uppfyller MB Sverige:s riktlinjer och krav för säkerhet och integritet innan ett lämpligt avtal ingås med ett underbiträde.

3. MODIFIERINGAR OCH VARIATIONER

Parterna kan uppdatera eller komplettera detta avtal i enlighet med den mekanism som överenskommit i det underliggande avtalet (villkoren för Use_ASP_B2B Connect).

4. AVTALSTID OCH UPSÄGNING

- 4.1 Detta avtal träder i kraft från och med båda parternas genomförande genom att acceptera dessa villkor elektroniskt (som en del av respektive villkor). Vardera parten i detta avtal ska vara bunden av villkoren i avtalet från och med den dag då parten vederbörligen har verkställt avtalet.
- 4.2 Detta avtal kommer att gälla så länge som avtalsförhållandet (som detta skyddsavtal är en del av) mellan parterna sägs upp eller tjänsterna upphör att tillhandahållas, beroende på vilken händelse som ligger längre fram i tiden, varvid det är underförstått att parternas skyldigheter enligt detta avtal kommer att fortsätta så länge som personuppgifter från den ena parten behandlas av den andra parten.

5. MEDDELANDEN

Alla meddelanden som ges enligt detta avtal ("**Meddelande**") ska ske skriftligen.

6. TILLDELNING

ASP får inte överlåta eller överföra några av rättigheterna eller skyldigheterna enligt detta avtal utan föregående skriftligt medgivande från MB Sverige.

7. Ansvar

Parterna ska vara ansvariga gentemot varandra för eventuella anspråk från tredje part eller andra förluster eller skador som de är ansvariga för (i synnerhet för skador som har uppstått inom deras respektive inflytandesfär) och som uppstår till följd av brott mot deras skyldigheter enligt detta avtal och/eller andra överträdelser av tillämpliga dataskyddslag, såvida inte den andra parten inte har fått kännedom om sådana skyldigheter. Om någon av parterna enligt Tillämplig dataskyddslagstiftning är skyldig att lämna full ersättning för den skada som den registrerade har

lidit och har gjort det, har sådan Part rätt att från den andra Parten återkräva den del av ersättningen som motsvarar den andra Partens andel av ansvaret för skadan.

8. SEPARERINGSKLAUSUL

- 8.1 Om någon bestämmelse i detta avtal skulle anses vara olaglig, ogiltig eller omöjlig att verkställa helt eller delvis, ska lagligheten, giltigheten och verkställbarheten av resten av detta avtal inte påverkas.
- 8.2 Parterna är överens om att komplettera den ogiltiga bestämmelsen vars effekt kommer så nära som möjligt det ekonomiska mål som parterna eftersträvar med den ogiltiga bestämmelsen. Ovanstående bestämmelser ska gälla i tillämpliga delar för det fall avtalet är ofullständigt.

9. TILLÄMPLIG LAG OCH JURISDIKTION

Platsen för fullgörandet är Malmö och jurisdiktion och jurisdiktionsort ska vara Malmö tingsrätt. Lagarna i Sverige ska tillämpas, med undantag för lagvalsregler. Parterna är överens om att utesluta tillämpningen av FN:s enhetliga köplag som bygger på FN:s konvention angående avtal om internationella köp av varor av den 11 april 1980 ("CISG").

10. FÖRHÅLLANDE TILL SEPARATA AVTAL

- 10.1 Detta avtal ersätter alla dataskyddsbestämmelser som tidigare fanns mellan parterna i förhållande till de databehandlingsaktiviteter som uttryckligen regleras häri.
- 10.2 Alla frågor som inte uttryckligen tas upp häri, inklusive parternas ansvar vid tillhandahållande eller användning av respektive tjänster eller överföring av respektive data för de angivna ändamålen, ska regleras av villkoren i eventuella ytterligare befintliga avtal (som härrör från avtalsförhållandet enligt avsnitt 4.2) mellan parterna.
- 10.3 I händelse av avvikelser mellan villkoren i detta avtal och sådana andra avtal som avses i avsnitt 10.2 ska villkoren i detta avtal ha företräde.

DEL A

KLAUSULER OM GEMENSAMT PERSONUPPGIFTSANSVAR

Förord

Inom ramen för sitt affärssamarbete inom B2B Connect vill parterna dela personuppgifter för vissa affärsändamål och behandla dem som personuppgiftsansvariga i den mening som avses i dataskyddslagstiftningen (nedan kallat "samarbete").

I dessa klausuler (nedan kallat "avtalet") fastställer parterna parternas rättigheter och skyldigheter med avseende på behandling av personuppgifter som utförs inom ramen för samarbetet och respektive ansvar när det gäller att uppfylla relevanta dataskyddsskyldigheter.

Mot denna bakgrund ingår parterna följande avtal:

1. Avtalets syfte

Detta avtal reglerar parternas (nedan även "personuppgiftsansvariga") rättigheter och skyldigheter vid behandling av personuppgifter i egenskap av gemensamt personuppgiftsansvariga.

2. Omfattning av behandling under Gemensam Kontroll

2.1 Under hela samarbetet behandlar parterna personuppgifter i egenskap av gemensamt personuppgiftsansvariga i den mening som avses i artikel 26 i GDPR. Bestämmelserna i detta avtal ska tillämpas på all behandling som utförs inom ramen för ett gemensamt personuppgiftsansvar där anställda hos de personuppgiftsansvariga eller personuppgiftsbiträden som de anlitat behandlar personuppgifter för de personuppgiftsansvarigas räkning. Omfattningen av behandlingen som gemensamt personuppgiftsansvarig, inklusive respektive roller, ansvar och befogenheter samt ytterligare detaljer om behandlingen, anges i bilaga 1.

2.2 Uppgifterna i bilaga 1 styrks av process- och verksamhetsbeskrivningarna i de avtal som parterna ingår parallellt (t.ex. tjänstekontrakt), inklusive de informationstexter som tillhandahålls parallellt, till vilka det hänvisas till dem.

3. De Personuppgiftsansvarigas Uppgifter

3.1 De personuppgiftsansvariga ska utföra behandlingen av personuppgifter i enlighet med relevanta bestämmelser i tillämpliga dataskyddslagar och ska vara gemensamt ansvariga för efterlevnaden av de GDPR-bestämmelser som är relevanta för gemensamt personuppgiftsansvariga med avseende på de behandlingsaktiviteter som omfattas av detta avtal och som anges i detta avtal. De ska särskilt se till att endast personuppgifter som är nödvändiga för den behandling och de ändamål som beskrivs i bilaga 1 samlas in. Dessutom ska de personuppgiftsansvariga följa principen om uppgiftsminimering (jfr. Artikel 5.1 c i GDPR).

3.2 Varje personuppgiftsansvarig är internt ansvarig för lagligheten av insamlingen och behandlingen av personuppgifter inom ramen för de uppgifter och ansvarsområden som tilldelats den nedan och i bilaga 1.

3.3 Personuppgiftsansvariga ska se till att alla personer som är involverade i behandlingen av personuppgifter inom ramen för samarbetet är eller kommer att vara bundna av sekretess- och datasekretessförpliktelser innan de får tillgång till sådana uppgifter, med verkan under deras verksamhet såväl som efter det att deras verksamhet har upphört. De ska se till att de berörda personerna instrueras om de dataskyddsbestämmelser som är relevanta för dem.

3.4 Personuppgiftsansvariga ska lagra personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format. Personuppgifterna ska vara korrekta och vid behov hållas uppdaterade. De personuppgiftsansvariga ska vidta alla åtgärder för att genomföra detta.

3.5 Personuppgiftsansvariga ska omedelbart och fullständigt informera varandra om de upptäcker fel eller oegentligheter med avseende på dataskyddsbestämmelser under granskningen av behandlingsaktiviteter.

3.6 Dokumentation som tjänar som bevis på korrekt behandling (jfr. Artikel 5.2 i GDPR) ska behållas av varje part i enlighet med dess rättsliga befogenheter och skyldigheter efter avtalets upphörande.

4. Tekniska och Organisatoriska Åtgärder

4.1 Med beaktande av den senaste tekniken, kostnaderna för genomförandet och behandlingens art, omfattning, sammanhang och ändamål, samt den varierande sannolikheten och allvaret i risken för fysiska personers rättigheter och friheter, ska personuppgiftsansvariga vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, i förekommande fall, följande:

- Förmågan att fortlöpande säkerställa konfidentialiteten, integriteten, tillgängligheten och motståndskraften hos de system och tjänster som är relaterade till behandlingen.
- förmågan att snabbt återställa tillgängligheten till och åtkomsten till personuppgifter i händelse av en fysisk eller teknisk incident;
- ett förfarande för att regelbundet granska, bedöma och utvärdera effektiviteten av de tekniska och organisatoriska åtgärderna för att säkerställa behandlingens säkerhet; och
- ett förfarande för korrekt efterlevnad av dataskyddsprinciperna med hjälp av teknik och genom dataskyddsvänliga standardinställningar i enlighet med (jfr. Artikel 25 i GDPR).

De Personuppgiftsansvariga kan specificera ytterligare krav separat.

4.2 De personuppgiftsansvariga ska vidta alla nödvändiga tekniska och organisatoriska åtgärder för att säkerställa att de registrerades rättigheter, särskilt enligt artikel 12 – 22 i GDPR, alltid kan utövas i enlighet med de rättsliga kraven. De personuppgiftsansvariga ska vid behov komma överens om den konkreta utformningen av åtgärderna och gemensamt besluta om genomförandet av dem.

4.3 Implementering, standardinställningar och drift av systemen ska utföras i enlighet med kraven i tillämpliga dataskyddslag, i synnerhet i enlighet med principerna om inbyggt integritetsskydd och integritetsskydd som standard, samt med hjälp av lämpliga tekniska och organisatoriska åtgärder i enlighet med den senaste tekniken.

5. Ansvar för efterlevnad av dataskyddslagar och registrerades rättigheter

5.1 Den registrerade kan hävda de rättigheter som den registrerade har rätt till enligt artikel 12–22 i GDPR gentemot någon av de personuppgiftsansvariga, som i princip förblir ansvariga för att respektive rättigheter uppfylls i den externa relationen.

5.2 Om inte annat anges i bilaga 1 eller i ett annat sammanhang, ska den personuppgiftsansvarige som ursprungligen samlade in de berörda personuppgifterna från den registrerade innan de överfördes till den andra personuppgiftsansvarige för vidare behandling, eller som hade eller har ett direkt avtalsförhållande med den registrerade, förbli den centrala kontaktpunkten för de registrerade och stödja den personuppgiftsansvarige som omfattas av GDPR med deras ansvar när det gäller fullgörandet av de registrerades rättigheter enligt artikel 12 – 22 GDPR i det interna förhållandet. Sådant stöd ska tillhandahållas på ett sätt som gör det möjligt för den andra personuppgiftsansvarige att fullt ut uppfylla dessa rättigheter.

5.3 De personuppgiftsansvariga kommer att stödja varandra i lämplig utsträckning för att uppfylla de registrerades rättigheter, informera varandra om motsvarande förfrågningar och förse varandra med all nödvändig information i god tid. Om personuppgifter ska raderas ska parterna underrätta varandra i god tid i förväg. Den andra parten kan invända mot raderingen av ett legitimt skäl, till exempel om den har en rättslig skyldighet att behålla uppgifterna.

5.4 Den registrerade ska få information om behandlingen i enlighet med artiklarna 13 och 14 i GDPR. De personuppgiftsansvariga ska stödja varandra i uppfyllandet av informationsskyldigheterna och förse varandra med nödvändig information om relevant databehandlingsverksamhet.

5.5 Om inte annat anges i bilaga 1 eller i ett annat sammanhang, ska den personuppgiftsansvarige som ursprungligen samlade in de berörda personuppgifterna från den registrerade innan de överfördes till den andra personuppgiftsansvarige för vidare behandling, eller som har haft eller har ett direkt avtalsförhållande med den registrerade, förbli ansvarig för att förse de registrerade med information om det huvudsakliga innehållet i dessa

bestämmelser. För detta ändamål kan den personuppgiftsansvarige på begäran förse de registrerade med bestämmelserna i detta avsnitt 6.

- 5.6 Var och en av de personuppgiftsansvariga ansvarar för rapporterings- och rapporteringsskyldigheterna till följd av potentiella dataintrång gentemot tillsynsmyndigheten och de registrerade som berörs av en personuppgiftsincident inom deras respektive ansvarsområde (jfr. Artikel 33 och 34 i GDPR). I händelse av en rapporteringspliktig incident med avseende på de behandlingsaktiviteter som omfattas av detta avtal ska de personuppgiftsansvariga informera varandra utan dröjsmål och innan incidenten rapporteras till en tillsynsmyndighet eller informerar de registrerade. De registeransvariga ska efter bästa förmåga stödja varandra när det gäller att klargöra fakta och vidta lämpliga åtgärder för att skydda de registrerade. Beslutet om nödvändigheten, innehållet och omfattningen av de åtgärder som ska vidtas ska fattas av respektive personuppgiftsansvarig som är skyldig att anmäla.
- 5.7 Parterna ska vid behov och på begäran bistå varandra vid utarbetandet av en konsekvensbedömning avseende dataskydd (jfr. Artikel 35 i GDPR) eller samråd med myndigheten (jfr. Artikel 36 i GDPR). Parterna skall i god tid förse varandra med den information som är nödvändig för detta inom sina respektive verksamhetsområden.
- 5.8 Varje personuppgiftsansvarig ska föra ett register över behandlingsaktiviteter på eget ansvar. Personuppgiftsansvariga ska förse varandra med den information som är nödvändig för att upprätthålla ett lämpligt register över behandlingen.
- 5.9 Dokument som tjänar som bevis på korrekt databehandling (se avsnitt 5.6) ska behållas av varje part efter avtalsförhållandets slut. Personuppgiftsansvariga ska se till att de uppfyller alla befintliga rättsliga skyldigheter att lagra de berörda personuppgifterna.
- 5.10 Om inget annat överenskommit ska varje personuppgiftsansvarig bära sina egna kostnader, om några, som uppstår vid fullgörandet av sina skyldigheter enligt detta avtal, utan att ha rätt att kräva någon ersättning från den andra administratören för fullgörandet av sådana skyldigheter.

6. Personuppgiftsbiträden

- 6.1 Varje Personuppgiftsansvarig har rätt att använda Personuppgiftsbiträden.
- 6.2 Om den Personuppgiftsansvarige anlitar ett personuppgiftsbiträde för den behandling som omfattas av detta Avtal ska detta endast ske i den utsträckning som kraven enligt Tillämplig Dataskyddslagstiftning ställer.
- 6.3 Personuppgiftsansvariga ska på begäran ge varandra tillgång till en förteckning över personuppgiftsbiträden som deltar i databehandlingsaktiviteter enligt detta avtal. De personuppgiftsansvariga ska på begäran informera de andra personuppgiftsansvariga om alla planerade ändringar som rör tillägg eller ersättning av andra personuppgiftsbiträden.
- 6.4 Detta gäller inte i de fall där den Personuppgiftsansvarige anlitar tredje part för tilläggstjänster. Dessa inkluderar, men är inte begränsade till, post-, telekommunikations-, frakt- och mottagningstjänster och fastighetsförvaltningstjänster. Personuppgiftsansvariga är fortfarande skyldiga att genomföra lämpliga avtalsarrangemang och skyldigheter med respektive tjänsteleverantör i enlighet med tillämpliga rättsliga krav och att vidta lämpliga kontrollåtgärder i förhållande till säkerheten för personuppgifter.

7. Behandling inom och utanför Europeiska ekonomiska samarbetsområdet

Behandlingen sker i princip i en medlemsstat i Europeiska unionen, i ett land inom Europeiska ekonomiska samarbetsområdet (EES) eller i ett land med en adekvat skyddsnivå. Behandling i andra länder utanför EES är tillåten, förutsatt att tillämpliga bestämmelser om internationell överföring av personuppgifter följs.

8. Ansvar

- 8.1 De Personuppgiftsansvariga är ansvariga gentemot de registrerade i enlighet med lagstadgade bestämmelser.
- 8.2 Personuppgiftsansvariga ska vara ansvariga i det interna förhållandet i den mån var och en av dem bär en del av ansvaret för den orsak som ger upphov till ansvar. Detta gäller även böter som åläggs en personuppgiftsansvarig för

brott mot dataskyddsbestämmelserna, förutsatt att den personuppgiftsansvarige först har uttömt alla rättsmedel mot myndighetsbeslutet. Om en personuppgiftsansvarig då förblir föremål för böter som inte motsvarar dess interna del av ansvaret för överträdelsen, är respektive annan personuppgiftsansvarig skyldig att hålla den berörda personuppgiftsansvarige skadeslös från böterna i den utsträckning som den bär ansvaret för den överträdelse som sanktioneras av böterna.

- 8.3 Eventuella ansvarsbegränsningar som överenskommit i tilläggsavtal för de aktuella tjänsterna ska gälla i enlighet med detta.

9. Fullmakt

- 9.1 MB Sverige har bemyndigats av MBAG att verkställa dessa klausuler om gemensamt Personuppgiftsansvar även i MBAG:s namn och på uppdrag av MBAG och därmed göra MBAG till en part i dessa klausuler om gemensamt personuppgiftsansvarig som en annan personuppgiftsansvarig med den roll som anges i bilaga 1. Om MBAG inte anges som registeransvarig i bilaga 1 nedan, ska MBAG inte bli part i detta avtal i detta avseende. ASP bekräftar och samtycker härmed till att MBAG blir en part enligt detta avtal och tilldelas alla rättigheter och skyldigheter som personuppgiftsansvarig enligt denna Del A inklusive dess bilagor (exklusive andra delar av avtalet om inte annat anges häri) och därmed blir personuppgiftsansvarig enligt detta avtal.
- 9.2 MB Sverige har rätt att informera MBAG om de ASP:er med vilka respektive avtalsförhållande har upprättats, inklusive företagsnamn, adress och innehåll i respektive avtal, och tillhandahålla tillräckliga bevis för detta på MBAG:s begäran, t.ex. genom att tillhandahålla kopior av det ingångna avtalet och denna Del A i synnerhet.

Bilaga 1: Roller, Uppgifter och Omfattning av Samarbetet

1. Affärsanalysrelaterade bearbetningsaktiviteter

Procedur	Syfte/Tillämpningsområde	Roller och uppgifter	Datakategorier och registrerade
<p>Ticket support för ISP i Seller Center</p>	<p>Ge ASP:er möjlighet att stödja ISP med Tickets i Seller Center och förfrågningar om kontoöppning.</p>	<p>MB Sverige: Kontrollant</p> <p>Ger ASP möjlighet att stödja ISP med tickets i Seller Center och gör information om ärenden och förfrågningar tillgängliga för ASP efter meddelande till ISP. ansvarar för den tekniska behandlingen av ticket information</p> <p>ASP: Kontrollant</p> <p>Stöder ticket / begäran om ISP i samarbete med ISP; ansvarar för att den information som lämnas hanteras på ett korrekt sätt och att den behandlas på rätt sätt</p>	<p>ISP data: ISPs företagsnamn, användarnamn, användar-ID, adress, e-postadress, telefon, ticket eller förfrågningsuppgifter (datum, ämne)</p> <p>ASP data: företagsnamn, användarnamn, användar-ID, adress, e-post, telefon</p>
<p>Business Analys</p>	<p>Försäljningsdata som erhållits genom driften av B2B Connect-plattformen ska användas för att analysera affärsverksamheten och för att tillhandahålla aggregerade rapporter till MBAG, MB Sverige och ASP.</p> <p>Rapporter skapas vanligtvis genom automatiserade beräkningar (applikationsbaserade).</p> <p>I undantagsfall slås data samman med data från andra källor (t.ex. en annan databas från en annan MBAG avdelning) för att köra ytterligare analys.</p> <p>MBAG och dess anställda arbetar strikt enligt principen om behovenlig behörighet.</p>	<p>MBAG: Kontrollant</p> <p>Driver affärslogik och är värd för databasen med affärsdata, skapar aggregerade utvärderingar/rapporter baserat på tillhandahållna data för sig själv, MB Sverige och ASP.</p> <p>MB Sverige: Kontrollant</p> <p>Gör det möjligt att överföra transaktionsrelaterade data från B2B-plattformen för ovanstående processer. tar emot aggregerade rapporter</p> <p>ASP: Kontrollant</p> <p>Gör det möjligt att överföra transaktionsrelaterade data från B2B-plattformen för ovanstående processer. tar emot aggregerade rapporter</p>	<p>ISP data: ISP:s företagsnamn, användarnamn, användar-ID, adress, e-post, telefon, beställningsinformation (beställningsdatum, beställda delar/tjänster, orderkvantitet, försäljning, ej gjorda beställningar (förlorad försäljning), användningsfrekvens för B2B Connect-plattformen/eftermarknadsrelaterade tjänster, leveranstider)</p> <p>ASP data: företagsnamn, användarnamn, användar ID, adress, e-post, telefon</p>

2. Mottagare

Begränsade personer med särskilda roller till vilka personuppgifter endast kommer att lämnas ut på behovsbasis som krävs för att de ska kunna utföra sina respektive ledningsuppgifter (t.ex. entreprenörer, inklusive de för HR, IT och ekonomi (i förekommande fall)); koncernföretag, konsulter, revisorer, bokförare, finansiella organisationer, brottsbekämpande myndigheter, statliga myndigheter, tillsynsmyndigheter.

DEL B

Klausuler om personuppgiftshantering på uppdrag av en personuppgiftsansvarig

Förord

Dessa klausuler om personuppgiftshantering för en personuppgiftsansvarigs räkning ("**Klausuler Del B**") specificerar parternas skyldigheter när det gäller dataskydd som följer av personuppgiftshantering för en personuppgiftsansvarigs räkning enligt beskrivningen nedan. Dessa klausuler i Del B gäller för all verksamhet som är relaterad till denna behandling och under vilken anställda hos personuppgiftsbiträdet eller tredje part som anlitas av personuppgiftsbiträdet kan komma i kontakt med den personuppgiftsansvariges personuppgifter. Dessa klausuler ska dock begränsas till omständigheter där en av parterna agerar som personuppgiftsbiträde i den mening som avses i artikel 28 GDPR gentemot den andra parten. Utanför detta tillämpningsområde ska dessa klausuler inte gälla.

1. Roller och ansvar

Den personuppgiftsansvarige förlitar sig på behandlingen av personuppgifter för att utföra sin eftermarknadsverksamhet. För detta ändamål tillhandahåller personuppgiftsbiträdet tjänster till den personuppgiftsansvarige enligt beskrivningen i Bilaga 1.

2. Syfte och ansvar

Personuppgiftsbiträdet behandlar personuppgifter för den personuppgiftsansvariges räkning. Föremålet för idrifttagningen är aktiviteter som specificeras nedan eller inom något ytterligare serviceavtal eller beställningsformulär. Inom ramen för dessa klausuler Del B ska den personuppgiftsansvarige vara ensam ansvarig för efterlevnaden av tillämplig dataskyddslagstiftning, i synnerhet lagligheten av överföringen av uppgifter till personuppgiftsbiträdet, behandlingen av uppgifterna genom personuppgiftsbiträdet och eventuell efterföljande behandling av uppgifter under tjänsternas gång, medan personuppgiftsbiträdet kommer att ansvara för att de lagstadgade bestämmelser om dataskydd som gäller för ett personuppgiftsbiträde följs.

3. Specifikation av idrifttagningen

- 3.1 Syfte, typ och omfattning av den uppdragna insamlingen, behandlingen och/eller användningen av personuppgifter beskrivs närmare i Bilaga 1.
- 3.2 Typen och kategorierna av de insamlade och/eller använda personuppgifterna samt den kategori av registrerade som är föremål för hanteringen av personuppgifter nedan beskrivs närmare i Bilaga 1.

4. Den Personuppgiftsansvariges rätt att ge anvisningar

- 4.1 Inom ramen för idrifttagningen förbehåller sig den personuppgiftsansvarige rätten att utfärda instruktioner om typen, omfattningen och förfarandet för databehandling som den kan specificera genom att utfärda individuella instruktioner. Dessa är slutgiltigt fastställda och ska utövas genom de inställningar och funktioner som tillhandahålls av de tillhandahållna applikationerna och systemen. Instruktioner som leder till ändringar av det överenskomna föremålet för behandlingen och förfarandena måste överenskommas och ska sedan dokumenteras.
- 4.2 Personuppgiftsbiträdet ska informera den personuppgiftsansvarige om alla instruktioner som den anser strida mot dataskyddskraven. Personuppgiftsbiträdet kan sedan skjuta upp utförandet av den relevanta instruktionen tills den har bekräftats eller ändrats av den personuppgiftsansvarige skriftligen (inkl. via e-post).
- 4.3 Med undantag för eventuella avvikande avtal mellan parterna har den personuppgiftsansvariges ledning eller annan behörig representant endast rätt att utfärda instruktioner från den personuppgiftsansvariges sida som ska vara skriftliga (inkl. via e-post).
- 4.4 Behörig att ta emot instruktioner från Personuppgiftsbitrådets sida är "Dataskyddssamordnaren för Mercedes-Benz Sverige AB" som kan kontaktas via legal_svedan@mercedes-benz.com.

5. Personuppgiftsbitrådets skyldigheter

- 5.1 Personuppgiftsbitrådet ska endast samla in eller behandla uppgifter på uppdrag av den Personuppgiftsansvarige och i enlighet med den Personuppgiftsansvariges instruktioner, såvida inte Personuppgiftsbitrådet är skyldigt att göra det enligt EU:s eller medlemsstaternas lagstiftning eller andra tillämpliga dataskyddslaggar som Personuppgiftsbitrådet omfattas av. Personuppgiftsbitrådet ska i sådant fall informera den Personuppgiftsansvarige om det rättsliga kravet innan behandlingen genomförs, såvida inte sådan information är förbjuden på grund av ett viktigt allmänintresse.

Personuppgiftsbitrådet kommer att korrigera, radera eller blockera de uppgifter som behandlas för den Personuppgiftsansvariges räkning endast enligt instruktioner från den Personuppgiftsansvarige. Om en registrerad kontaktar Personuppgiftsbitrådet med en begäran om rättelse eller radering av sina uppgifter ska Personuppgiftsbitrådet vidarebefordra begäran till den Personuppgiftsansvarige.

- 5.2 Såvida det inte är förbjudet enligt tillämplig lag eller en juridiskt bindande begäran från brottsbekämpande myndigheter, ska Personuppgiftsbitrådet omedelbart meddela den Personuppgiftsansvarige om varje begäran från en tillsynsmyndighet för dataskydd, brottsbekämpande myndighet eller annan offentlig myndighet om tillgång till eller beslagtagande av personuppgifter. Dessutom, i den utsträckning det är tillåtet enligt lag, ska registerföraren använda alla rimligen tillgängliga åtgärder för att försvara sig mot sådana åtgärder eller tillåta den Personuppgiftsansvarige att göra det i stället för och på uppdrag av Personuppgiftsbitrådet, och om den så önskar, ansöka om en skyddsorder eller tillåta den Personuppgiftsansvarige att göra det på Personuppgiftsbitrådets vägnar. Under alla omständigheter ska Personuppgiftsbitrådet rimligen samarbeta med den Personuppgiftsansvarige i ett sådant försvar.
- 5.3 Innan Personuppgiftsbitrådet beviljar tillgång till Personuppgifter ska Personuppgiftsbitrådet ålägga personer som är anställda vid behandling av Personuppgifter datasekretess och konfidentialitet och bekanta dem med bestämmelserna i dessa Klausuler Del B och de dataskyddsskyldigheter som gäller för dem. I den mån Personuppgiftsbitrådet behandlar personuppgifter som omfattas av tystnadsplikt eller andra särskilda sekretessförpliktelser (t.ex. uppgifter som omfattas av telekommunikationssekretess) ska en sådan skyldighet även omfatta dessa särskilda omständigheter och relaterade skyldigheter.
- 5.4 I den utsträckning som krävs enligt Tillämplig Dataskyddslagstiftning ska Personuppgiftsbitrådet utse ett dataskyddsbud och vidarebefordra dennes kontaktuppgifter till den Personuppgiftsansvarige och utan onödigt dröjsmål rapportera till den Personuppgiftsansvarige om eventuella ändringar och uppdateringar under detta Avtals giltighetstid.
- 5.5 Personuppgiftsbitrådet ska utan onödigt dröjsmål underrätta den Personuppgiftsansvarige om Personuppgiftsbitrådet eller en person som är anställd av Personuppgiftsbitrådet bryter mot instruktioner eller bestämmelser om skydd av den Personuppgiftsansvariges personuppgifter.

Personuppgiftsbitrådet är införstådd med att den Personuppgiftsansvarige kan vara skyldig att dokumentera överträdelser av skyddet av personuppgifter och, om nödvändigt, informera en tillsynsmyndighet, respektive den registrerade, inom 72 timmar om en sådan överträdelse. Om och i den mån det har skett sådana överträdelser ska Personuppgiftsbitrådet bistå den Personuppgiftsansvarige i enlighet med artikel 28 para. 3 lit. f GDPR med efterlevnad av sina rapporteringsskyldigheter på ett korrekt sätt för att göra det möjligt för den personuppgiftsansvarige att i tid fullgöra sina skyldigheter enligt detta avtal. Personuppgiftsbitrådet ska informera den Personuppgiftsansvarige om överträdelsen utan onödigt dröjsmål och ge åtminstone följande information om och i den utsträckning som Personuppgiftsbitrådet har tillgång till: a) Beskrivning av vilken typ av incident det rör sig om, kategori och det ungefärliga antalet registrerade och dataset som berörs. b) Namn på och kontaktuppgifter till en kontaktperson för ytterligare information. c) Beskrivning av de sannolika konsekvenserna av incidenten. d) Beskrivning av de åtgärder som vidtagits för att avhjälpa eller minska överträdelsen.

Personuppgiftsbitrådet ska dessutom utan onödigt dröjsmål informera den Personuppgiftsansvarige om allvarliga störningar i den normala verksamheten, eventuella misstankar om dataskyddsoverträdelser eller andra oegentligheter vid behandlingen av den Personuppgiftsansvariges uppgifter.

- 5.6 Personuppgiftsbitrådet ska informera den Personuppgiftsansvarige om tillsynsmyndighetens eventuella övervakningsaktiviteter och åtgärder som vidtas med avseende på den Personuppgiftsansvariges behandling av Personuppgifter.

- 5.7 Personuppgiftsbiträdet bistår den Personuppgiftsansvarige i enlighet med artikel 28 paragraf. 3 lit. e GDPR genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt och rimligt, för att uppfylla den Personuppgiftsansvariges skyldighet gentemot de registrerade, (inklusive enligt kapitel II i GDPR), t.ex. information till och tillgång till de registrerade, rättelse och radering av uppgifter, begränsning av behandling eller rätten till dataportabilitet och rätt att göra invändningar, i tillämpliga fall.
- 5.8 Personuppgiftsbiträdet hjälper till i enlighet med artikel 28 para. 3 lit. f GDPR med utarbetandet av en konsekvensbedömning avseende dataskydd enligt artikel 35 GDPR och, i förekommande fall, bistår med föregående samråd med tillsynsmyndigheten enligt artikel 36 GDPR. På den Personuppgiftsansvariges begäran ska Personuppgiftsbiträdet lämna ut den information och de handlingar som krävs till den Personuppgiftsansvarige.
- 5.9 Parterna ska komma överens om eventuella tillkommande kostnader som uppkommer enligt 5.7 och 5.8 ovan. Det finns ingen skyldighet att bära kostnaderna för sådana tjänster som MB Sverige utför och som MB Sverige är eller skulle vara skyldig att utföra, oavsett om det finns ett sådant uppdrag enligt lag.
- 5.10 Personuppgiftsbiträdet ska övervaka efterlevnaden av de skyldigheter som anges ovan under utförandet av den beställda databehandlingen.
- 5.11 Registerföraren ska föra ett register över behandlingsaktiviteter som utförs för den Personuppgiftsansvariges räkning.

6. Säkerhet vid Behandling

- 6.1 Personuppgiftsbiträdet vidtar alla lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken och bistå den Personuppgiftsansvarige med att säkerställa efterlevnad av tillämpliga dataskyddslagar.

Inom ramen för sitt ansvarsområde kommer Personuppgiftsbiträdet således att inrätta sin interna organisation i enlighet med alla tillämpliga krav på dataskydd och datasäkerhet. Personuppgiftsbiträdet ska vidta, upprätthålla och kontrollera tekniska och organisatoriska åtgärder för att säkerställa lämpligt skydd av den Personuppgiftsansvariges uppgifter mot missbruk och förlust i enlighet med kraven i tillämpliga lagar.

- 6.2 I detta sammanhang ska registerföraren tillhandahålla en säkerhetsnivå som är lämplig i förhållande till risken, med beaktande av den senaste tekniken, kostnaderna för genomförandet och behandlingens art, omfattning, sammanhang och ändamål samt risken för varierande sannolikhet och allvarlighetsgrad för fysiska personers rättigheter och friheter. Detta inbegriper lämpliga åtgärder för t.ex. tillträdeskontroll, användarkontroll, åtkomstkontroll, överföringskontroll, inmatningskontroll, jobbkontroll, tillgänglighetskontroll samt separering efter syfte och, bland annat när så är lämpligt, pseudonymisering och kryptering av personuppgifter, förmågan att säkerställa fortlöpande konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystem och tjänster, förmågan att återställa tillgängligheten och åtkomsten till personuppgifter i tid i händelse av en fysisk eller teknisk incident och en process för att regelbundet testa, bedöma och utvärdera effektiviteten av tekniska och organisatoriska åtgärder för att säkerställa behandlingens säkerhet.
- 6.3 Ytterligare specifikationer om de tekniska och organisatoriska åtgärderna finns i [Bilaga 2](#).
- 6.4 Tekniska och organisatoriska åtgärder är beroende av tekniska framsteg och utveckling. Personuppgiftsbiträdet får vidta lämpliga alternativa åtgärder. Dessa får dock inte underskrida den säkerhetsnivå som de angivna åtgärderna ger. Eventuella väsentliga förändringar måste dock dokumenteras.

7. Den personuppgiftsansvariges rättigheter och skyldigheter

- 7.1 Personuppgiftsansvarig och Personuppgiftsbiträde ska var och en ansvara för att respektive lagstadgad dataskyddslag som gäller för den ena eller den andra med avseende på de personuppgifter som ska behandlas enligt denna lag.
- 7.2 Registrerade kommer att ha olika rättigheter med avseende på de personuppgifter som innehas av den Personuppgiftsansvarige (och Personuppgiftsbiträdet för dennes räkning). Eftersom det i vilket fall som helst också kommer att vara den Personuppgiftsansvarige som har en direkt relation med den registrerade, ska den Personuppgiftsansvarige se till att de relevanta registrerades rättigheter uppfylls på ett korrekt sätt, i synnerhet för att på ett korrekt sätt informera de registrerade om de roller och uppgifter som utförs av parterna i enlighet med tillämpliga dataskyddslagar, t.ex. genom att ge kunderna tillgång till den faktiska versionen av den relevanta integritetspolicyn.

7.3 Den Personuppgiftsansvarige ska specificera åtgärderna för återlämnande av tillhandahållna datamedier och/eller radering av inspelade data efter att idrifttagningen har avslutats. Om inga specifikationer utfärdas ska uppgifterna överlämnas till den personuppgiftsansvarige eller förstöras. I den mån uppgifter raderas i enlighet med särskilda specifikationer ska registerföraren bekräfta sådan radering till den Personuppgiftsansvarige och ange det datum då sådan radering har utförts på begäran av den Personuppgiftsansvarige.

8. Revision

8.1 Den Personuppgiftsansvarige eller dennes utsedda representant har rätt att kontrollera efterlevnaden av alla instruktioner och krav som anges i detta avtal samt enligt tillämplig dataskyddslag, inklusive regelbundna inspektioner. Personuppgiftsbiträdet åtar sig att tillåta sådana kontroller och att stödja den Personuppgiftsansvarige samt tillhandahålla nödvändig information.

8.2 Den Personuppgiftsansvarige ska i första hand fullfölja sina kontrollskyldigheter genom att kräva respektive egenkontroll av dataskyddsombudet i Personuppgiftsbitrådets dataskyddsorganisation och/eller certifiering av oberoende revisorer. Den Personuppgiftsansvarige förbehåller sig rätten att utföra ytterligare inspektioner på plats om det är nödvändigt enligt tillämplig dataskyddslagstiftning.

8.3 Revisioner av den Personuppgiftsansvarige i enlighet med avsnitt 8.1 och 8.2 ovan ska äga rum under ordinarie kontorstid, får inte störa den normala interna verksamheten och meddelas i rimlig tid i förväg.

8.4 På den Personuppgiftsansvariges skriftliga begäran ska Personuppgiftsbiträdet inom rimlig tid förse den Personuppgiftsansvarige med all information och göra dokumentationen tillgänglig i den utsträckning som krävs för granskningen.

9. Underbiträden

9.1 Personuppgiftsbiträdet ska ha rätt att använda underbiträden för att uppfylla sina avtalsförpliktelser.

9.2 Personuppgiftsbiträdet ska genom att ingå avtal med underbiträden säkerställa att de ålägger underbiträden åtminstone i huvudsak samma skyldigheter som Personuppgiftsbiträdet har åtagit sig enligt dessa klausuler i Del B innan underbiträdet beviljas tillgång till den Personuppgiftsansvariges personuppgifter under utförandet.

9.3 I den mån Personuppgiftsbiträdet involverar underbiträden innehåller Bilaga 1 ytterligare information om de berörda underbiträdena per förfarande. Dessutom förtecknas berörda underbiträden i Bilaga 3. Personuppgiftsbiträdet ska informera den Personuppgiftsansvarige om alla planerade ändringar som rör tillägg eller ersättning av andra underbiträden, och därigenom ge den Personuppgiftsansvarige möjlighet att invända mot sådana ändringar, medan den Personuppgiftsansvarige måste lägga fram rimliga skäl för en sådan invändning. Om den Personuppgiftsansvarige fortfarande inte godkänner ett nytt underbiträde kan den personuppgiftsansvarige och Personuppgiftsbiträdet säga upp de berörda delarna av tjänsterna utan påföljd genom att tillhandahålla ett skriftligt meddelande om uppsägning.

9.4 Detta avsnitt 9 ska inte gälla i de fall där registerföraren lägger ut tilläggstjänster på underentreprenad till tredje part. Sådana kompletterande tjänster ska omfatta, men inte begränsas till, post-, kommunikations-, transport- och mottagningstjänster samt vaktmästeritjänster.

10. Territoriella och internationella dataöverföringar

10.1 Som en allmän regel ska behandlingen ske i en medlemsstat i Europeiska unionen, i ett land inom Europeiska ekonomiska samarbetsområdet eller i ett adekvat land. Behandling i ett annat land ("Tredjeland") ska tillåtas om de tillämpliga kraven för internationell överföring av Personuppgifter är uppfyllda.

10.2 I den mån internationella dataöverföringar (i förekommande fall, inklusive dataöverföringar i förhållande till underentreprenörer) inte omfattas av Mercedes-Benz dataskyddspolicy EU A 17.4 ska parterna (även i förhållande till underentreprenörer) ingå respektive EU standardavtalsklausuler.

10.3 I tillämpliga fall ska villkoren i EU:s standardavtalsklausuler (inklusive dess bilagor) ha företräde framför eventuella motstridiga klausuler i resten av dessa klausuler del B och hela avtalet. För att undvika missförstånd ska bestämmelser i resten av dessa klausuler del B samt hela avtalet som endast går utöver villkoren i EU:s standardavtalsklausuler utan att motsäga dem förbli giltiga.

11. Ansvar

Utan att det påverkar tillämpningen av avsnitt 7 i huvuddelen av detta avtal ska den Personuppgiftsansvarige vara skadeståndsansvarig och ska hålla Personuppgiftsbiträdet skadeslös mot eventuella anspråk från tredje part eller andra skador och ansvar, inklusive konsekvenserna av tillsynsmyndigheters beslut eller böter, till följd av (i) den Personuppgiftsansvariges brott mot sina skyldigheter enligt detta avtal och/eller andra överträdelser av tillämpliga dataskyddslagar, och/eller (ii) Personuppgiftsbitrådets brott mot tillämpliga dataskyddslagar, i den mån dessa grundar sig på ett korrekt genomförande av bestämmelserna i detta Avtal eller andra instruktioner från den Personuppgiftsansvarige. Detta gäller inte om den Personuppgiftsansvarige inte är ansvarig för de omständigheter som ger upphov till ansvar.

Bilaga 1: Roller, Uppgifter och Omfattning av Samarbetet

1. B2B Connect Platform relaterade behandlingsaktiviteter

Procedur	Syfte/Tillämpningsområde	Roller och uppgifter	Datakategorier och registrerade
Systemstöd för B2B Connect Platform tjänster	Tillhandahålla användarsupport till anställda på ASP (via ärendeverktyg/callcenter)	<p>MB Sverige: Processor (MBAG: Underbiträde)</p> <p>Ger stöd till ASP respektive</p> <p>ASP: Kontrollant</p> <p>Använda WebParts, inklusive användarsupport</p>	<p>ASP material: kontouppgifter inklusive kundnamn/företagsnamn, kundens anställdas namn och kundens kontaktuppgifter, kundadress, supportticket/incidentrelaterad information, information om eftermarknadstjänster, systemanvändningsdata, inklusive transaktionsdata och relaterade ISP data, inklusive ISP företagstitel, anställdas namn eller inköpsorderrelaterade data (vid behov)</p>

2. Business Analys

Procedur	Syfte/Tillämpningsområde	Roller och uppgifter	Datakategorier och registrerade
Visning, rapportering och analys	Visa ISP transaktionsdata i B2B Connect Seller Center, tillhandahålla rapporter och analyser	<p>MB Sverige: Processor (MBAG: Underbiträde)</p> <p>Visar ISP transaktionsdata i B2B Connect Seller Center och tillhandahåller rapporter och analyser på begäran av ASP</p> <p>ASP: Kontrollant</p> <p>Använd WebParts, inklusive datavisning, rapportering och analys</p>	<p>ISP data: ISP företagsnamn, användarnamn, användar ID, orderinformation (beställningsdatum, beställda delar/tjänster, orderkvantitet, försäljning, ej gjorda beställningar (förlorad försäljning), användningsfrekvens för B2B Connect plattformen/eftermarknadsrelaterade tjänster, leveranstider), analyser och rapporter baserade på ovanstående försäljningssiffror</p> <p>ASP material: företagsnamn, användarnamn, användar ID</p>
Kampanjförslagstjänster (om en sådan tjänst efterfrågas av MB Sverige och/eller ASP; annars inte tillämpligt)	MBAG och MB Sverige (i förekommande fall) använder tillhandahållna data för att köra affärsanalyser och skapa relaterade marknadsföringskampanjer för MB Sverige och ASP och för att hjälpa till med att driva marknadsföringskampanjer. Detta innebär vanligtvis att MBAG tillhandahåller marknadsföringsmaterial, inklusive ISP listor (t.ex. med leads) till MB Sverige eller ASPs för att göra det möjligt för dem att kontakta ISP:er via olika direktmarknadsföringskanaler (om tillämpligt på den specifika	<p>MBAG: Processor</p> <p>Är värd för databasen med affärsanalyser; driver applikationer och skapar marknadsföringskampanjer baserade på de data som tillhandahålls för MB Sverige och ASP för att göra det möjligt för dem att kontakta ISP via olika direktmarknadsföringskanaler. Överför marknadsföringsmaterial + ISP listor till MB Sverige och/eller ASPs för detta ändamål.</p> <p>MB Sverige: Kontrollant</p>	<p>ISP data: ISP:s företagsnamn, användarnamn, användar-ID, adress, e-post, telefon, beställningsinformation (beställningsdatum, beställda delar/tjänster, orderkvantitet, försäljning, ej gjorda beställningar (förlorad försäljning), användningsfrekvens för B2B Connect-plattformen/eftermarknadsrelaterade tjänster, leveranstider)</p> <p>BSP-material: företagsnamn, användarnamn, användar-ID, adress, e-post, telefon</p>

	marknaden), inklusive överföring av marknadsföringsmaterial + återförsäljarlistor till MB Sverige eller ASPs för detta ändamål.	<p>Ta emot ISP listor + marknadsföringsmaterial för marknadsföringskampanjer (marknadsföringskampanjer kommer att drivas av MB Sverige på eget ansvar, om tillämpligt)</p> <p>Kan tillhandahålla liknande tjänster som ASP (i detta fall även agera som personuppgiftsbiträde för ASP)</p> <p>ASP: Kontrollant</p> <p>Ta emot ISP-listor + marknadsföringsmaterial för marknadsföringskampanjer (marknadsföringskampanjer kommer att drivas av ASP på eget ansvar)</p>	
Kampanjtjänster för direktmarknadsföring (om en sådan tjänst begärs av ASP; annars inte tillämpligt)	Alternativt kan MB Sverige, på beställning av en ASP, stödja utskick av marknadsföringsmaterial till kunder genom att tillhandahålla en dedikerad webbtjänst där ASP kan ladda upp slutkundens kontaktuppgifter och MB Sverige kan distribuera kampanjer i ASP:s namn och för dess räkning. MB Sverige kan också stödja ASP med marknadsföringstjänster genom att kontakta ISP via MB callcenter	<p>MB Sverige: Processor</p> <p>MB Sverige kan komma att skicka ut marknadsföringskampanjer (e-post) i ASP:s namn och för dess räkning (eller involvera MBAG eller annan underentreprenör för den delen). I detta fall tillhandahåller MB Sverige ett gränssnitt via vilket ASP kan överföra uppgifter om slutkunder (namn, e-postadress) till MB Sverige.</p> <p>MB Sverige kommer då att behandla de överförda uppgifterna för att skicka ut marknadsföringsmeddelanden via e-post (även via tredjepartsleverantörer av MB Sverige).</p> <p>Alternativt kan MB Sverige kontakta ISP via MB:s callcenter och följa upp tidigare affärstransaktioner</p> <p>ASP: Kontrollant</p> <p>Driver marknadsföringskampanjer</p>	<p>ASP data: företagsnamn, medarbetarens namn, användar-ID, adress, e-post, telefon</p> <p>ISP data: företagsnamn, kontaktuppgifter, anställdas namn, e-post, orderinformation (beställningsdatum, beställda delar/tjänster, orderkvantitet, försäljning, ej gjorda beställningar (förlorad försäljning), användningsfrekvens för B2B Connect-plattformen/eftermarknadsrelaterade tjänster, ytterligare leadrelaterad information</p>

3. Mottagare

Begränsade personer med särskilda roller till vilka personuppgifter endast kommer att lämnas ut på behovsbasis som krävs för att de ska kunna utföra sina respektive ledningsuppgifter (t.ex. entreprenörer, inklusive de för HR, IT och ekonomi (i förekommande fall)); koncernföretag, konsulter, revisorer, bokförare; finansiella organisationer, brottsbekämpande myndigheter, statliga myndigheter, tillsynsmyndigheter.

Bilaga 2: Tekniska och Organisatoriska Åtgärder

Följande tekniska och organisatoriska åtgärder "TOM" återspeglar de åtgärder som implementeras i de enskilda funktionella komponenterna i den relevanta miljön. Beroende på underfunktion och tillämpning kan det hända att inte alla de åtgärder som anges nedan genomförs fullt ut (t.ex. särskilda åtkomstkontrollåtgärder för applikationer som redan används i särskilt skyddade miljöer, t.ex. särskilt skyddade datacenter). Specifika detaljerade beskrivningar av de tekniska och organisatoriska åtgärder som vidtagits för varje produktkomponent, delfunktion eller (del)tillämpning kommer att göras tillgängliga på begäran.

För B2B Connect relaterade behandlingsaktiviteter (inklusive affärsanalys och kampanj-/marknadsföringsupport) ska följande TOM:er gälla:

1. Åtkomstkontroll (fysisk)	Ja	Nej	Ej tillämpligt
De områden med system där applikationer behandlar personuppgifter är indelade i olika säkerhetszoner	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Specifikation av behöriga personer, inklusive behörighetsområde avseende fysisk tillgång till relevanta rum eller områden	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Utfärdade auktoriserings ID:n för godkännande	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ordningsregler för besökare på plats	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regler och föreskrifter för implementerade nycklar	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alla individer registrerade in och ut	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fysiskt skydd av företagets lokaler (t.ex. staket, ytterväggar, kontrollpunkter)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Säker entré (t.ex. låssystem, ID läsare)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Inbrottssäkra fönster	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Övervakningsinstallation (t.ex. larmsystem, CCTV)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separeringssystem (t.ex. vändkors, dubbel dörrsystem)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dokumentation av fysiska skyddsåtgärder	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Åtkomstkontroll (system)	Ja	Nej	Ej tillämpligt
Dokumenterat säkerhetskoncept för att komma in i (inloggning) applikationen	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Användning av Global Authentication Service (GAS)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regelbunden synkronisering med företagskatalogen	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Användning av säker Application Gateway (SAGW/WCP)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Åtkomstbehörighet specificerad och kontrollerad	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Användaren har identifierats och auktoriseringen har verifierats	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hanteringssystem för användaridentitet implementerat	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Särskild autentiseringsprocess (t.ex. chipkort, biometrisk åtkomstkontroll)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Lämpligt lösenordsskydd (bindande krav på säkra lösenord, krypterad lagring)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Övervakade åtkomstförsök, inklusive svar på säkerhetsproblem	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Isolering av internt nätverk (t.ex. med hjälp av VPN, brandväggar)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Omedelbar radering av tidigare anställdas konton	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Särskild säkerhetsprogramvara (t.ex. skydd mot skadlig kod, intrångsdetektering)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ordningsregler för besökare på plats	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regler och föreskrifter för fjärråtkomst	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Åtkomstkontroll (användarrättigheter)	Ja	Nej	Ej tillämpligt
Auktoriserings- och rollkoncept implementerat för program	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Användarkonton som krävs för dataåtkomst	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regelbunden översyn av tillstånd	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Åtkomstbegränsningar som införts (baserat på principerna om behovsinformation och minsta behörighet)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ytterligare lösenord (baserat på 4-eyes-principen) för särskilt viktiga funktioner (t.ex. systemadministratör)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Säkerställande av systemets kapacitet för flera klienter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separerade databaser som kan användas för flera klienter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separering av utvecklings-, test-, integrations- och produktionsmiljö	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separering av produktions- och arkiveringsmiljö	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Loggad läsbehörighet	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Loggad skrivåtkomst	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Obehöriga åtkomstförsök loggas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Genomförande av lagringstider för uppgifter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Kontroll av offentliggörande	Ja	Nej	Ej tillämpligt
Dataöverföring krypterad	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Datalagring krypterad	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Krypterade mobila terminaler (t.ex. hårddiskkryptering)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Loggning av vidarebefordran eller överföring av data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fullständigt dokumenterade former av vidarebefordran av uppgifter (t.ex. utskrifter, datamedier, automatisk överföring)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Dokumenterade gränssnitt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Begränsning av rättigheter för dataöverföring	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rimlighets-, fullständighets- och korrekthetskontroller av utförda uppgifter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Inaktivering av USB gränssnitt	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Regler för hantering av mobila enheter implementerade	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Implementerade bestämmelser om bortskaffande av databärare	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Skydd mot datamanipulation (skydd mot skadlig kod)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5. Kontroll av indata	Ja	Nej	Ej tillämpligt
Systemloggning/registrering säkerställd	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regelbunden utvärdering av loggfiler/protokoll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ansvarsfördelning (SoD) säkerställd (SoD-matris definierad och förfaranden genomförda)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dokumenterad behörighet att lägga in, ändra eller radera uppgifter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Inmatning/ändring av uppgifter som loggats/registrerats fullständigt	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Registrering/ändring av uppgifter som delvis registrerats/registrerats	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ändring/radering av uppgifter förbjuden	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Elektronisk signatur för att säkerställa äktheten av dataändringar	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

6. Kontroll över jobbet	Ja	Nej	Ej tillämpligt
Mercedes-Benz standardavtal om databehandling för Mercedes-Benz räkning har ingåtts	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Personuppgiftsbitrådets standardavtal om databehandling för uppdrag har överenskommit	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
EU kommissionens standardavtalsklausuler har överenskommit för databehandling på uppdrag av personuppgiftsbitråden i tredje land	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Personuppgiftsansvarigas och personuppgiftsbitrådets ansvar är strikt reglerade/separerade	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regler specificerade för att justera/ändra instruktioner som ges till personuppgiftsbitrådet	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kontroller på plats har utförts och dokumenterats av den personuppgiftsansvarige	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Personuppgiftsbitrådet har lämnat in självutvärderingar	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Personuppgiftsbiträde inlämnade godkända certifieringar	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Personuppgiftsbiträde lämnade in lista över underleverantörer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kontroll av underleverantörer per personuppgiftsbiträde	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

7. Kontroll av tillgänglighet	Ja	Nej	Ej tillämpligt
Systemets skick kontrolleras regelbundet (övervakning)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Säkerhetskopierings- och återställningsplan på plats (regelbunden säkerhetskopiering av data)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Strategi för dataarkivering implementerad	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dokumenterade beredskapsplaner (affärskontinuitet, haveriberedskap)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Beredskapsplaner testas regelbundet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Förekomst av redundanta IT system (servrar, lagring osv.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fullt fungerande fysiska skyddssystem på plats (brandskydd, energi, luftkonditionering)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8. Förfaranden för regelbunden översyn, bedömning och utvärdering av effektiviteten hos de tekniska och organisatoriska åtgärder som vidtagits	Ja	Nej	Ej tillämpligt
Regelbundna kontroller av systemets status (övervakning)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Översyn av genomförandet av de beskrivna åtgärderna	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Beskrivning av tillämpliga dataskyddskrav i bindande riktlinjer och instruktioner för åtgärder	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dataskyddsombudets deltagande i relevanta nya förfaranden för behandling av uppgifter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

För Webparts relaterade bearbetningsaktiviteter (inklusive affärsanalys och kampanj-/marknadsföringsupport) ska följande TOM:er gälla:

1. Åtkomstkontroll (fysisk)	Ja	Nej	Ej tillämpligt
De områden med system där applikationer behandlar personuppgifter är indelade i olika säkerhetszoner	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Specifikation av behöriga personer, inklusive behörighetsområde avseende fysisk tillgång till relevanta rum eller områden	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Utfärdade auktoriserings- ID:s för godkännande	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ordningsregler för besökare på plats	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regler och föreskrifter för implementerade nycklar	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Alla individer registrerade in och ut	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fysiskt skydd av företagets lokaler (t.ex. staket, ytterväggar, kontrollpunkter)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Säker entré (t.ex. låssystem, ID-läsare)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Inbrottssäkra fönster	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Övervakningsinstallation (t.ex. larmsystem, CCTV)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separeringssystem (t.ex. vändkors, dubbeldörrsystem)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dokumentation av fysiska skyddsåtgärder	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2. Åtkomstkontroll (system)	Ja	Nej	Ej tillämpligt
Dokumenterat säkerhetskoncept för att komma in i (inloggning) applikationen	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Användning av Global Authentication Service (GAS)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regelbunden synkronisering med företagskatalogen	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Användning av säker Application Gateway (SAGW/WCP)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Åtkomstbehörighet specificerad och kontrollerad	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Användaren har identifierats och auktoriseringen har verifierats	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hanteringssystem för användaridentitet implementerat	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Särskild autentiseringsprocess (t.ex. chipkort, biometrisk åtkomstkontroll)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lämpligt lösenordsskydd (bindande krav på säkra lösenord, krypterad lagring)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Övervakade åtkomstförsök, inklusive svar på säkerhetsproblem	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Isolering av internt nätverk (t.ex. med hjälp av VPN, brandväggar)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Omedelbar radering av tidigare anställdas konton	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Särskild säkerhetsprogramvara (t.ex. skydd mot skadlig kod, intrångsdetektering)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ordningsregler för besökare på plats	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regler och föreskrifter för fjärråtkomst	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Åtkomstkontroll (användarrättigheter)	Ja	Nej	Ej tillämpligt
Auktoriserings- och rollkoncept implementerat för program	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Användarkonton som krävs för dataåtkomst	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regelbunden översyn av tillstånd	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Åtkomstbegränsningar som införts (baserat på principerna om behovsinformation och minsta behörighet)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Ytterligare lösenord för särskilt viktiga funktioner (t.ex. systemadministratör)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Säkerställande av systemets kapacitet för flera klienter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separerade databaser som kan användas för flera klienter	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Separering av utvecklings-, test-, integrations- och produktionsmiljö	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Separering av produktions- och arkiveringsmiljö	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Loggad läsbehörighet	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Loggad skrivåtkomst	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Obehöriga åtkomstförsök loggas	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Genomförande av lagringstider för uppgifter	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

4. Kontroll av offentliggörande	Ja	Nej	Ej tillämpligt
Dataöverföring krypterad	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Datalagring krypterad	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Krypterade mobila terminaler (t.ex. hårddiskkryptering)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Loggning av vidarebefordran eller överföring av data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fullständigt dokumenterade former av vidarebefordran av uppgifter (t.ex. utskrifter, datamedier, automatisk överföring)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dokumenterade gränssnitt	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Begränsning av rättigheter för dataöverföring	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rimlighets-, fullständighets- och korrekthetskontroller av utförda uppgifter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Inaktivering av USB gränssnitt	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Regler för hantering av mobila enheter implementerade	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Implementerade bestämmelser om bortskaffande av databärare	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Skydd mot datamanipulation (skydd mot skadlig kod, Malware)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

5. Kontroll av indata	Ja	Nej	Ej tillämpligt
Systemloggning/registrering säkerställd	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Regelbunden utvärdering av loggfiler/protokoll	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ansvarsfördelning (SoD) säkerställd (SoD matris definierad och förfaranden genomförda)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dokumenterad behörighet att lägga in, ändra eller radera uppgifter	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Inmatning/ändring av uppgifter som loggats/registrerats fullständigt	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Registrering/ändring av uppgifter som delvis registrerats/registrerats	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ändring/radering av uppgifter förbjuden	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Elektronisk signatur för att säkerställa äktheten av dataändringar	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

6. Kontroll över jobbet	Ja	Nej	Ej tillämpligt
Mercedes-Benz standardavtal om databehandling för Mercedes-Benz räkning har ingåtts	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Personuppgiftsbitrådets standardavtal om databehandling för uppdrag har överenskommit	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EU-kommissionens standardavtalsklausuler har överenskommit för databehandling på uppdrag av personuppgiftsbiträden i tredje land	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Personuppgiftsansvarigas och personuppgiftsbitrådets ansvar är strikt reglerade/separerade	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Regler specificerade för att justera/ändra instruktioner som ges till personuppgiftsbiträdet	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kontroller på plats har utförts och dokumenterats av den personuppgiftsansvarige	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Personuppgiftsbiträdet har lämnat in självvärderingar	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Personuppgiftsbiträde inlämnade godkända certifieringar	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Personuppgiftsbiträde lämnade in lista över underleverantörer	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kontroll av underleverantörer per personuppgiftsbiträde	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

7. Kontroll av tillgänglighet	Ja	Nej	Ej tillämpligt
Systemets skick kontrolleras regelbundet (övervakning)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Säkerhetskopierings- och återställningsplan på plats (regelbunden säkerhetskopiering av data)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Strategi för dataarkivering implementerad	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dokumenterade beredskapsplaner (affärskontinuitet, haveriberedskap)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Beredskapsplaner testas regelbundet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Förekomst av redundanta IT system (servrar, lagring osv.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fullt fungerande fysiska skyddssystem på plats (brandskydd, energi, luftkonditionering)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

8. Förfaranden för regelbunden översyn, bedömning och utvärdering av effektiviteten hos de tekniska och organisatoriska åtgärder som vidtagits	Ja	Nej	Ej tillämpligt
Regelbundna kontroller av systemets status (övervakning)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Översyn av genomförandet av de beskrivna åtgärderna	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Beskrivning av tillämpliga dataskyddskrav i bindande riktlinjer och instruktioner för åtgärder	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Dataskyddsombudets deltagande i relevanta nya förfaranden för behandling av uppgifter	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Bilaga 3: Underbiträden

#	<i>Subprocesor till MB Sverige inklusive adress/plats</i>	<i>Föremålet för och behandlingens art</i>	<i>Varaktighet</i>
1.	Mercedes-Benz Group AG	Teknisk drift av B2B Plattform + tillhandahållande av användarsupport	Under terminen använder sig ASP av B2B

Bilaga 2: Regler för Plattformen

1. Allmänna Regler för Plattformen

MB Sverige förbehåller sig rätten att blockera Partners eller Kunder (nedan gemensamt benämnda "Användare" eller "Användaren") eller vidta andra lämpliga åtgärder i händelse av tecken på felaktig användning av B2B Connect eller användning som bryter mot gällande avtalsbestämmelser. I synnerhet ska sådan felaktig användning anses olämplig om Användaren använder B2B Connect eller information som tillhandahålls däri för andra ändamål än de avsedda ändamålen, använder B2B Connect för ändamål som är olagliga eller kränker MB Sverige:s eller tredje parts rättigheter, eller använder B2B Connect i strid med andra riktlinjer som tillhandahålls av MB Sverige.

Användaren garanterar att all information som lämnas till MB Sverige och andra användare alltid är sanningsenlig, korrekt och fullständig och i enlighet med alla rättsliga krav och tillämpliga avtalsbestämmelser. Användaren förbinder sig att utan dröjsmål informera MB Sverige om eventuella framtida väsentliga ändringar av den information som lämnas till MB Sverige och som är relevanta för avtals- eller användarförhållandet.

I synnerhet får B2B Connect inte användas för spridning av innehåll som uppfyller något av följande kriterier: rasistiska, omänskliga slagord; tillhandahållande av falsk eller på annat sätt felaktig information; information som är stötande, kränkande, trakasserande, hatisk, obscen, hotfull eller på annat sätt stötande; innehåll som strider mot rättsliga krav eller där tillämpliga krav inte iakttas eller genomförs i tillräcklig utsträckning (t.ex. när det gäller märknings- eller transparenskrav); innehåll vars tillhandahållande eller spridning utgör ett brott eller en förseelse och innehåll vars tillhandahållande eller spridning utgör ett brott eller en administrativ förseelse.

Om information eller innehåll som lämnats till MB Sverige strider mot de gällande användarvillkoren för B2B Connect och MB Sverige får kännedom om det (t.ex. genom en anmälan från en kund eller annan tredje part) förbehåller sig MB Sverige rätten att omedelbart (vid behov även tillfälligt) blockera eller radera motsvarande information eller innehåll och att vidta alla ytterligare nödvändiga åtgärder.

Om det är nödvändigt eller lämpligt kommer följande åtgärder att vidtas beroende på överträdelsens allvarlighetsgrad, frekvens och antal:

- tillfällig eller permanent radering av innehåll;
- tillfällig blockering av ett användarkonto eller användaråtkomst;
- inaktivering av användarkontot eller användaråtkomsten i 3 månader;
- permanent blockering av användarkontot och allt tillhörande innehåll;
- permanent blockering av användarkontot och allt tillhörande innehåll samt åtkomstdata, i synnerhet kommer den angivna e-postadressen och andra masterdata för att identifiera användaren att svart listas med följden att ett nytt användarkonto eller innehåll inte kan skapas;

I den utsträckning som krävs enligt lag kommer Användaren att informeras om MB Sverige:s beslut och ges möjlighet att kommentera beslutet. Därefter, eller om inga sådana kommentarer lämnas, kommer MB Sverige att ompröva beslutet och fatta ett slutgiltigt beslut om hur det berörda innehållet ska hanteras. Beroende på det enskilda fallet kommer ytterligare modereringsåtgärder som finns beskrivna i de relevanta användarvillkoren för B2B Connect att tillämpas. Användaren kommer att få ett meddelande/e-postmeddelande om modereringsbeslutet inklusive en motivering till beslutet.

Kommentarer rörande modereringsbeslutet eller begäran om modereringsbeslut enligt lagen om digitala tjänster kan lämnas till de kontaktpunkter som nämns i avsnitt 3.2. Användaren måste specificera vilket beslut som denne hänvisar till (t.ex. genom att ange datum, ämne och/eller ärendenummer) och vad denne invänder mot beslutet eller vill få förklarad mer detaljerat.

Klagomål som inte kan lösas genom de processer beskrivits ovan kan lämnas in till och behandlas av ett certifierat organ för tvistlösning utanför domstol. Vid behov kommer information om tillgång till ett sådant certifierat organ för tvistlösning utanför domstol att göras tillgänglig på B2B-webbplatsen under "rättsligt meddelande". Oberoende av om ett sådant organ är inblandat eller inte är det alltid möjligt att vända sig till behöriga domstolar.

2. Identifiering av kommersiellt innehåll och reklam innehåll

När användare tillhandahåller andra Användare inom B2B Connect information och innehåll måste det i enlighet med gällande lagar framgå att det rör sig om kommersiella erbjudanden och reklam.

I samband med reklam erbjudanden måste Användarna tillhandahålla klar och tydlig information om annonsören. Detta inkluderar till exempel i vilket namn annonsen visas och vem som har betalat för annonsen.

Om reklam erbjudanden visas för olika användare eller användargrupper, beroende på användar- eller användargruppens beteende eller liknande (särskilt vid inriktning eller profilering), måste användaren tillhandahålla klar och tydlig information om de relevanta parametrarna som avgör vilken sådan information som ska visas för andra användare eller användargrupper. Användaren måste alltid hålla all information uppdaterad.

MB Sverige kommer så långt det är möjligt att tillhandahålla tekniska lösningar och möjligheter inom B2B Connect med vilka Användaren kan fullgöra sina respektive skyldigheter. Om inga sådana tekniska lösningar presenterats eller om dessa inte är tillräckliga ur Användarens synvinkel, ska MB Sverige omedelbart informeras om detta och parterna ska omedelbart samordna genomförandet av motsvarande åtgärder.

3. Kontaktpunkter

För frågor om innehållet på B2B Connect kan Användaren använda de kontaktpunkter som denne hittar på B2B webbplatsen under "Leverantör/datasekretess". Vid kontakt med MB Sverige ska Användaren alltid specificera sin förfrågan genom att ange vad dennes förfrågan avser, varför denne kontaktar MB Sverige i detta avseende och hur MB Sverige kan hjälpa Användaren med dennes förfrågan.

3.1 Olagligt innehåll

Om Användaren vill rapportera olagligt innehåll och överträdelser av de tillämpliga användarvillkoren för B2B Connect ska Användaren använda kontaktformuläret som finns på B2B webbplatsen under "Leverantör/datasekretess". Vid kontakt med MB Sverige ska Användaren alltid specificera sin förfrågan genom att t.ex. ange varför Användaren anser att ett visst innehåll är olagligt eller bryter mot vissa bestämmelser, var sådant innehåll kan hittas, när Användaren hittade det etc.).

3.2 Klagomål på och frågor om beslut

Om Användaren vill kontakta MB Sverige med ett klagomål på ett beslut som fattats och som går emot denne enligt ovan, ska Användaren använda kontaktformuläret som finns på B2B webbplats under "Leverantör/Dataskydd".
