

이용 약관

B2B Connect Seller Center 및 WebParts Dealer Client의 공식 서비스 파트너용

MBK(메르세데스벤츠코리아 주식회사 및 서울특별시 중구 한강대로 416, 9층) (이하 "MBK")와 B2B Connect에 참여하는 공식 서비스 파트너(이하 "파트너") 및 관련 서비스 (B2B Connect Seller Center and WebParts Dealer Client)를 "B2B Connect"라고 통칭합니다.

이러한 맥락에서 고객은 자동차 수리 및 유지 보수 서비스를 수행하는 B2B(Business) 독립 기업가(예: 개별 서비스 제공업체 및 차량 고객)(이하 "고객"이라고 함)입니다.

MBK 및 파트너는 이하 "당사자"라고 합니다.

서문

B2B Connect는 MBK에서 제공합니다. B2B 커넥트는 B2B 커넥트 셀러 센터(메르세데스-벤츠 애프터세일즈 에코시스템에서 이용 가능)를 통한 메르세데스-벤츠 순정부품 판매와 관련 시장에서 이용 가능한 한 다른 하위 시스템을 통해 고객에게 제공되는 수리 및 유지 보수 솔루션을 통합하는 기술 에코시스템입니다. 파트너의 경우 B2B Connect와 관련된 서비스는 WebParts Dealer Client 및 B2B Connect Seller Center를 통해 제공됩니다. WebParts Dealer Client의 기능은 이후에 B2B Connect Seller Center로 마이그레이션됩니다.

고객은 자체 등록을 통해 B2B Connect에 액세스할 수 있으며 데이터를 사용자 지정할 수 있는 반면, B2B Connect를 통한 Mercedes-Benz 순정 부품의 온라인 주문은 WebParts 딜러 클라이언트의 파트너가 수락 및 활성화한 후(B2B Connect Seller Center에서 마이그레이션한 후)에만 사용할 수 있습니다.

현재 WebParts Dealer Client 및 B2B Connect Seller Center의 목표는 A/S 비즈니스의 경쟁력과 수익성 향상뿐만 아니라 A/S (OTC 비즈니스)의 마케팅 도구로서 파트너에게 인터넷에서 고객 중심의 체계적인 솔루션을 제공하는 것입니다. 승인된 서비스 계약의 조항은 본 이용 약관에도 적용됩니다.

주문 프로세스에 대한 고객 데이터는 WebParts Dealer Client를 통해 파트너에게 표시되며 향후 B2B Connect Seller Center를 통해 파트너에게 표시되며 파트너의 관리 시스템으로 가져올 수 있습니다.

§ 1 시스템 요구 사항

파트너의 부품 가용성을 고객에게 표시하려면 파트너는 MBK가 MBAG와 협력하여 제공하는 Logistikbus에 연결되어 있어야 합니다. 그렇지 않으면 정보의 가용성이 제한됩니다.

§ 2 MBK 서비스, 계약 체결, 변경, 참여 및 5*평가자

MBK는 파트너 고객을 위해 순정 부품을 온라인으로 주문할 수 있는 파트너 B2B Connect Seller Center 및 WebParts Dealer Client를 제공합니다.

MBK에서 제공하는 B2B Connect Seller Center 및 WebParts Dealer Client를 통해 파트너는 다음을 수행할 수 있습니다.

- 활성화된 고객을 참조하십시오.
- 정가를 조정하고,
- 할인율을 정의하고,
- 자신의 고객 할인 코드를 정의하고,
- 선택한 고객 할인 코드를 할당하고,
- 자신의 할인 그룹을 정의하고,
- 도착 예정 시간에 관한 정보 정의
- 고객 요청 지원
- 5*Rate를 통해 고객으로부터 제품, 서비스 및 전반적인 성과에 대한 피드백을 받습니다.
- B2B Connect with Customers를 통해 실행된 거래와 관련된 정보(예: 고객 이름, 주문 관련 정보 등)를 기반으로 맞춤형 캠페인 제안 및 캠페인 지원 서비스를 받습니다.
- B2B Connect 및 PartsLink24에서 주문 요청 및 고객 거래 관리

B2B Connect에 참여할 때 고객은 5*Rate를 통해 파트너의 제품, 서비스 및 전반적인 성과를 평가할 수 있습니다. B2B Connect, Seller Center 및 WebParts Dealer, Client Partner에 참여하고 이를 사용함으로써 클라이언트 파트너는 고객 피드백이 제공되고 MBK가 이 정보를 집계된 형식(특정 거래와 관련된 정보를 포함하지 않음)으로 수신하며, 시장 및 파트너 성과 검토 및 전반적인 성과 조정 및 파트너와의 협업을 위해 이 정보를 사용할 수 있다는 사실을 인정하고 수락합니다. 이러한 맥락에서 개인 데이터 사용과 관련된 자세한 내용은 본 이용 약관의 **부록 1**에 명시되어 있습니다.

고객이 입력한 데이터를 기반으로 고객은 인터넷을 통해 파트너로부터 주문할 수 있으며, 이를 통해 고객별 가격과 각 Mercedes-Benz 순정 부품의 재고가 표시됩니다. 이를 위한 전제 조건은 고객이 B2B Connect에 등록하고 WebParts Dealer Client의 파트너가 고객을 활성화하는 것입니다. 고객 주문은 B2B Connect를 통해 파트너에게 전송됩니다. 파트너는 표준 내보내기 형식을 통해 읽을 수 있으며 파트너의 관리 시스템으로 가져올 수 있습니다.

파트너는 주문 수락 여부와 접수된 주문 중 수락하고자 하는 주문을 자유롭게 선택할 수 있습니다. 파트너와 고객이 반대되는 계약을 체결하지 않은 경우, 파트너가 주문 수락을 전달하여 고객의 주문을 수락하는 시점에 계약이 체결된 것으로 간주됩니다. B2B Connect를 통한 계약 이행은 해당 파트너의 전적인 책임 하에 있는 문제입니다. B2B Connect를 통해 관리되는 계약과 관련하여 MBK는 B2B Connect를 통해 파트너와 고객 간에 체결된 계약의 이행에 대해 어떠한 보증도 하지 않습니다. MBK는 파트너사와 고객 간에 체결된 계약의 이행을 보장할 어떠한 의무도 부담하지 않습니다.

MBK는 B2B Connect를 통해 제공되는 기능을 변경할 수 있으며, 이러한 변경으로 인해 본 이용 약관을 변경할 필요가 없습니다. MBK는 별도의 합의가 없는 한 변경 최소 1개월 전에 서면 형식(예: 이메일)으로 파트너에게 통지해야 합니다.

달리 합의하지 않는 한, MBK는 언제든지 파트너에게 중립적이거나 이익이 되는 범위 내에서 본 이용 약관을 개정할 수 있습니다. 그렇지 않은 경우, MBK는 변경 사항이 발생하기 최소 6주 전에 텍스트 형식으로 파트너에게 통지해야 합니다. 파트너가 그러한 통지를 받은

후 4주 이내에 텍스트 형식의 변경에 이의를 제기하지 않는 경우, 제안된 변경 사항은 통지 후 6주 후에 당사자에게 구속력을 갖습니다. MBK는 이러한 변경에 대해 이의를 제기하지 않는 것의 효력을 제휴사에 통지와 함께 통지해야 합니다. 파트너는 이러한 변경에 이의를 제기할 권리가 있습니다. 파트너가 이의를 제기하는 경우, MBK는 정당한 사유로 인해 변경의 영향을 받는 파트너의 서비스 이용을 종료할 수 있습니다.

MBK가 WebParts Dealer Client를 B2B Connect Seller Center에 직접 통합하는 경우 위의 규정에 따라 이러한 맥락에서 구현될 수 있는 본 이용 약관의 필요한 개정에 따라 본 이용 약관이 계속 적용됩니다.

§ 3 B2B Connect Seller Center 및 WebParts Dealer Client 사용

파트너는 WebParts Dealer Client를 통해 온라인 주문을 위해 활성화할 수 있는 관심 있는 고객을 받습니다. 활성화는 부당한 지연 없이 이루어져야 합니다.

계약상의 판매 제한 사항(특히 공인 서비스 계약 및 표준)을 준수하는 것은 파트너의 책임입니다.

마스터 데이터(예: 자체 정의된 고객 할인 클래스에 대한 할인율 정의, 자체 정의된 할인 그룹 또는 캠페인에 대한 Mercedes-Benz 순정 부품 할당 등)는 파트너가 시스템에 입력해야 합니다.

파트너는 가격 책정, 할인 부여 및 고객 할인 라벨링에 있어 자유롭습니다. 가격, 할인, 고객할인 코드 또는 캠페인은 고객이 주문을 설정할 때 고객에게 표시되며 데이터를 최신 상태로 유지하는 것은 파트너의 책임입니다.

파트너는 고객에 대한 일반 이용 약관 및 데이터 보호 규정을 WebParts Dealer Client에 게시하고 필요한 범위 내에서 해당 동의를 얻어야 합니다. 파트너의 일반 이용 약관에는 파트너가 순정 부품의 판매자임을 충분히 명확하게 명시해야 합니다. 데이터 보호 규정은 파트너가 주문 수행과 관련하여 고객의 데이터와 관련하여 관리자임을 충분히 명확하게 명시해야 합니다. 또한 파트너의 데이터 보호 규정은 각각 적용되는 데이터 보호법(정보 의무 포함), 특히 일반 데이터 보호 규정(GDPR)의 법률을 준수해야 합니다. 본 이용 약관 기간 중 언제든지 파트너가 해당 데이터 개인 정보 보호법에 따라 순정 부품을 제공할 수 없는 경우 파트너는 MBK에 알려야 합니다. 파트너는 MBK가 요구하는 합리적인 기간 내에 치료법을 제안할 수 있습니다. 파트너가 제안한 솔루션이 MBK에 합리적으로 수용되지 않는 경우, MBK는 본 이용 약관의 전부 또는 일부를 즉시 종료할 권리가 있습니다.

B2B Connect의 목적은 순정 부품과 관련된 파트너의 제안을 온라인으로 프레젠테이션하는 것입니다. 고객은 이 목적으로만 B2B Connect를 사용할 수 있습니다.

B2B Connect의 사용은 본 이용 약관에 따른 사용 권한 외에 B2B Connect, 사용된 URL 또는 함께 제공되는 문서(매뉴얼, 가이드 투어 등)에 대한 어떠한 권리도 부여하지 않습니다.

파트너는 워크 스테이션 컴퓨터, 태블릿, 라우터, 데이터 통신 시스템 등을 포함하여 적용 가능한 범위 내에서 B2B Connect Seller Center 및 WebParts Dealer Client를 사용하는 데 사용하는 하드웨어 및 소프트웨어에 바이러스, 웜, 트로이 목마 등이 없는지 확인할 것을 약속합니다. 파트너가 업로드한 모든 데이터와 관련하여 파트너는 업로드된 데이터에 대한 모든 권리의 소유자임을 보장하고 업로드된 데이터가 그러한 사용에 반대하는 제3자의 권리에 저촉되지 않도록 포함하여 해당 사용에 대해 자유롭게 처분할 수 있음을 보장합니다.

파트너는 고객의 요청 시 B2B Connect 판매자 센터를 통해 MBK에 대한 불만 사항 또는 B2B Connect와 관련된 기타 요청을 고객에게 지원할 수 있습니다. 이러한 지원은 무료로 제공되며(MBK에 대한 보상 또는 비용 또는 경비의 상환을 청구할 권리가 없음) 파트너의 B2B Connect 판매자 센터 사용 또는 고객에게 제공되는 추가 지원에 대해 MBK가 어떠한 책임도 지지 않고 고객 자신의 책임 및 관계 하에서만 제공됩니다. 이는 파트너가 고객에게 제공하는 기타 거래 관련 정보(예: 예상 도착 시간에 대한 정보)를 WebParts Dealer Client에서 제공하는 경우에도 적용됩니다.

§ 4 데이터 흐름

고객은 B2B Connect에서 자체 등록을 통해 데이터를 입력합니다. 이 데이터는 공급자 MBK에 의해 인증되고 저장됩니다. 데이터는 B2B Connect Seller Center의 파트너에게도 제공됩니다.

§ 5 기밀 유지

양 당사자는 B2B Connect 사용과 관련하여 본 이용 약관 기간 동안 직접 또는 간접적으로 액세스할 수 있는 고객의 사용 데이터를 포함한 모든 기술 및 경제 정보를 기밀로 취급해야 합니다. 이러한 데이터는 계약 이행에 필요하거나 여기에 달리 규정된 경우 및 해당 제3자와 해당 기밀 유지 계약이 있는 경우에만 MBK가 제3자에게 액세스할 수 있습니다. 파트너에 의해 활성화된 고객 데이터 또는 고객 사용 데이터는 MBK가 본 이용 약관의 이행을 위해서만 사용하며, Mercedes-Benz AG는 플랫폼 개발을 위해 익명화합니다.

기밀 정보로 분류되지 않는 정보 및 문서는 다음과 같습니다.

- 일반적으로 알려진 정보 또는 본 이용 약관에 포함된 의무를 위반하지 않고 알려지게 된 정보,
- 당사국이 자체 업무의 일환으로 검증 가능하게 작성하거나 획득한 정보, 또는
- MBK가 제3자로부터 합법적으로 제공받은 정보입니다.

당사자는 법적 규정 또는 관할 당국의 처분으로 인해 정보를 공개해야 하는 경우 정보를 기밀로 취급할 의무가 면제됩니다.

§ 6 데이터 보호

B2B Connect를 통한 순정 부품/서비스에 대한 판매 및 판매 프로세스와 관련하여 당사자는 독립적인 관리자 간에 관련 개인 데이터를 교환하고자 하는 반면, MBK는 B2B Connect 운영을 위한 개인 데이터 처리의 컨트롤러가 됩니다. 달리 규정되지 않는 한, 당사자는 일반적으로 고객의 개인 데이터에 대한 개별 처리와 관련하여 공동 통제권을 설정할 의도가 없습니다. MBK, Mercedes-Benz AG(및/또는 그 계열사) 및/또는 파트너 간의 관계가 GDPR 제26조에 따라 공동 관리자로서의 자격을 갖추거나 자격을 갖추는 경우, 양 당사자는 GDPR 제26조에 따라 공동 관리자의 책임을 규정하는 적절한 공동 관리자(들)와 향후 적절한 공동 관리자 계약을 체결하거나 체결하는 데 동의합니다.

MBK는 파트너 및 파트너 고객의 개인 데이터를 (i) 처리자로서 파트너를 대신하여, (ii) 5*Rate에서 개인 데이터를 사용하는 경우, B2B Connect Seller Center를 통한 지원 또는 비즈니스 분석 및 마케팅 캠페인 서비스를 위해 컨트롤러로 처리합니다. 당사자 간에 합의된 데이터 보호에 관한 조항은 본 이용 약관의 **부록 1**에 명시되어 있습니다.

§ 7 데이터 품질, 파트너의 의무

파트너는 WebParts 딜러 클라이언트를 통해 순정 부품을 제공/표시하는 데 필요한 정보(가격, 할인, 재고, 배송 시간 등)를 최신 상태로 유지할 책임이 있습니다.

파트너는 고객이 순정 부품을 주문했는지 여부를 온라인 또는 전자적 수단으로 통지 후 정기적으로 확인합니다. 파트너는 이러한 주문을 딜러 관리 시스템으로 내보내고 계속 처리합니다. 파트너는 적절한 시간 내에 주문을 처리하고 고객에게 주문 상태를 알립니다. 고객이 요청한 배송 기한을 준수할 수 있는지 여부에 대한 고객에 대한 주문 확인은 기존 방식으로 수행해야 합니다.

MBK는 적절한 액세스 보호 시스템을 제공하며, 요청 시 파트너에게 액세스 권한을 부여합니다. 파트너는 시스템에 액세스할 때 적절한 애플리케이션 사용을 포함하여 직원이 시스템을 적절하게 사용하도록 보장할 것을 약속합니다. 파트너는 자신에게 할당된 액세스 권한을 권한이 없는 사람에게 공개하지 않을 것을 약속합니다. 파트너는 적절한 시간 내에 고객의 등록 수락 요청에 응답하고 WebParts 딜러 클라이언트에 대한 MBK 1차 및 2차 수준 지원을 제공할 것을 약속합니다. MBK는 파트너의 조직 단위 및 고객의 사용자 ID 및 비밀번호 오용에 대해 어떠한 책임도 지지 않습니다.

MBK는 부적절한 사용의 징후가 있는 경우 해당 사용자를 차단할 권리가 있습니다. 파트너는 이에 대해 직접 통보를 받습니다.

B2B Connect는 전 세계에서 사용할 수 있는 기술 솔루션입니다. 파트너는 B2B Connect의 순정 부품에 대한 판매 및 판매 프로세스와 관련하여 해당 국가의 해당 법률 프레임워크 조건을 정기적으로 확인할 책임이 있으며, MBK는 B2B Connect 운영에 대한 해당 법적 프레임워크 조건을 정기적으로 확인할 책임이 있습니다.

특히 파트너는 본 이용 약관에 규정된 서비스를 제공하기 위해 고객과 관련된 모든 요구 사항(필요한 동의 및 정보 포함)이 충족되는지 확인해야 합니다.

§ 8 가용성

현재 기술 상태로 인해 B2B Connect의 제공 및 사용은 MBK가 통제할 수 없는 특정 제한 및 부정확성의 영향을 받을 수 있습니다. 이는 특히 인터넷 액세스의 가용성에 적용됩니다. 파업, 직장 폐쇄 또는 당국의 명령을 포함한 불가항력으로 인해 중단이 발생하거나 B2B Connect가 적절하게 제공되거나 개선되도록 하기 위해 MBK 시스템 또는 서비스 제공업체의 시스템에서 수행해야 하는 기술 또는 기타 조치(예: 수리, 유지 보수, 소프트웨어 업데이트 및 개선)로 인해 중단이 발생할 수도 있습니다.

§ 9 책임, 면책

MBK와 제휴사는 고의 및 중과실의 경우 본인 및 대리인에 대한 책임을 지며, 사망 또는 신체 상해의 경우 경미한 과실에 대해서도 책임을 집니다.

또한, MBK와 파트너사는 다음과 같은 경미한 과실에 대해 책임을 집니다. 책임은 필수적인 계약상의 의무를 위반한 경우에만 구성됩니다. "필수 계약상 의무"는 이러한 의무의 이행이 계약의 적절한 이행을 위해 필수적으로 중요한 경우(기본 의무)입니다. 이 책임은 계약 체결 당시 예측 가능한 일반적인 직접 손해로 제한됩니다. 해당 손해에 대해 파트너 또는 MBK가 체결한 보험 증권(전체 보험 제외)에 의해 손해가 보장되는 한, MBK 또는 파트너는 보험이 확정될 때까지 보험료 인상 또는 이자율 불이익과 같은 파트너 또는 MBK의 관련 불이익에 대해서만 책임을 집니다.

제휴사는 본 약관 및 본 약관에서 고려되는 거래(제휴사의 판매자 센터 이용을 포함하되 이에 국한되지 않음)의 과실로 인한 위반으로 인해 발생하는 모든 손해, 손실, 책임, 청구(제3자 청구 포함) 및 비용(적절한 변호사 수임료 및 비용 포함)으로부터 MBK를 면책할 의무가 있습니다.

§ 10 이용 약관의 기간 및 종료

본 이용 약관은 2023년 부터 동일한 주제와 관련된 이전 이용 약관을 대체하며 수락과 함께 시작됩니다.

양 당사자는 서면으로 본 이용 약관을 해지할 수 있으며(§ 10에 따른 모든 해지와 관련하여 텍스트 형식으로 충분함) 3개월부터 월말까지 통지 기간을 둘 수 있습니다. 어떤 경우든 본 이용 약관은 당사자 간의

승인된 서비스 계약이 종료되는 것으로 종료됩니다.

이용 약관이 종료된 후에도 § 4, 5 및 6에 언급된 데이터 보호 및 기밀 유지에 대한 조항은 계속 존재합니다.

§ 5에 따른 기밀 유지 의무 위반을 구성하는 데이터 전송과 같이 본 이용 약관을 심각하게 위반하는 경우, 각 당사자는 통지 없이 본 이용 약관을 해지할 수 있습니다. 일방 당사자의 심각한 계약 위반으로 인해 계약이 해지되는 경우, 상대방은 추가 손해를 주장할 권리가 있습니다.

주 라이선스가 중단된 경우 종료: WebParts Dealer Client 및 B2B Connect Seller Center를 파트너에게 제공할 수 있는 MBK 권한은 MBAG와 MBK 간의 계약에서 파생됩니다. MBK는 WebParts Dealer Client 및 B2B Connect Seller Center를 제공할 수 있는 자체 권리가 MBAG에 의해 종료/지속되지 않는 경우 파트너에게 사전 서면 통지를 통해 본 이용 약관을 해지할 수 있습니다.

§ 11 세금

파트너가 제공하는 WebParts 딜러 클라이언트 및 B2B Connect 판매자 센터에 게시된 제품 또는 파트너가 B2B Connect에 게시하고 고객에게 제공한 서비스(예: 디지털 서비스 세금)에 대해 MBK가 정당하게 할당한 세금 및 관세를 납부할 의무가 있는 경우, 파트너는 해당 세금 및 관세로 인해 발생하는 MBK의 모든 비용을 부담합니다. MBK가 부담하는 부가가치세와 납부하지 않은 부가가치세에도 동일하게 적용됩니다.

§12 관할 구역

본 이용 약관은 대한민국 법률의 적용을 받습니다. 본 약관으로 인해 발생하는 분쟁에 대한 배타적 관할권은 대한민국입니다.

이 이용 약관의 부록

부록 1 - 데이터 보호 계약

부록 1:

데이터 보호 계약

B2B Connect 플랫폼 및 관련 서비스

사이

메르세데스-벤츠 코리아 (Mercedes-Benz Korea Ltd.)

서울특별시 중구 한강대로 416

("MBK")

그리고

공식 서비스 파트너

("ASP")

(각각 "당사자", 총칭하여 "양 당사자").

배경

- (A) MBK 는 Mercedes-Benz Company 그룹의 회사이며 독일, 유럽(EU) 및 기타 국가("RoW")의 딜러(ISP 고객(이하 "ISP") 및 공식 서비스 파트너를 포함한 "딜러")와 관련하여 특정 애프터세일즈 및 마케팅 관련 서비스(이하 "서비스", 아래에 정의됨)를 제공하여 Mercedes-Benz AG 의 비즈니스를 지원합니다.
- (B) **반면**, 서비스 제공 및 제공에는 ASP 에 서비스를 제공하기 위해 MBK 에 대한 개인 데이터 전송 및 처리가 포함됩니다.
- (C) **반면**, 유럽 및 현지 데이터 보호법은 무엇보다도 회사 그룹, 유통 또는 애프터 서비스 네트워크 내에서 개인 데이터를 전송 및 처리하는 것과 관련된 특정 요구 사항을 규정합니다.
- (D) **반면**, 본 계약은 아래에 정의된 관련 데이터 보호법에 따라 개인 데이터의 국가적, 국경 간, EU 전체 및 전 세계 전송 및 처리 과정에서 적절한 보호 장치 및 보호를 제공하기 위한 것입니다.
- (E) **따라서** 양 당사자는 다음과 같은 계약(이하 "계약")을 체결합니다.

1. 정의

1.1 본 계약에서 다음 용어는 다음과 같은 의미를 갖습니다.

- (a) "개인 데이터", "컨트롤러", "처리자", "처리/처리", "데이터 주체", "기술적 및 조직적 조치" 및 "감독 기관/권한"은 GDPR 또는 관련 데이터 보호법에 따른 동등한 용어에 따라 해석되어야 합니다. 하위 처리자는 GDPR 의 "다른 처리자" 또는 관련 데이터 보호법에 따른 동등한 용어와 동일한 의미를 갖습니다.
- (b) ""계약"은 본 데이터 보호 계약을 의미합니다.
- (c) "관련 데이터 보호법"은 GDPR, 유럽 연합 회원국에 적용되는 국가 데이터 보호법 또는 본 계약에 따라 데이터를 처리할 때 각 당사자에게 공동으로 또는 개별적으로 적용되는 기타 국가 데이터 보호법을 의미합니다. 한 당사자가 이에 따라 본 계약을 체결했다는 사실이 한 당사자에게 적용되는 데이터 보호법이 다른 당사자에게 자동으로 적용되거나 그 반대의 경우도 마찬가지라는 영향을 미치지 않습니다. 본 계약의 조건에 따라 당사자에 대한 해당 데이터 보호법의 적용 가능성은 해당 법률에 따라 결정됩니다. 따라서 본 계약에 명시된 당사자의 추가 조항 및 의무에 따라 각 당사자는 적용되는 경우에만 해당 데이터 보호법을 준수해야 합니다. 예를 들어, GDPR 12-22 조에 따른 데이터 주체의 법적 권리 또는 GDPR 28 조에 따른 데이터 처리에 대한 법적 요구 사항을 언급하는 경우, 이러한 권리 또는 요구 사항은 GDPR 의 범위에 속하는 컨트롤러에만 적용됩니다.
- (d) "적절한 국가"는 유럽연합 집행위원회(European Commission)가 국내법 또는 체결한 국제적 약속에 따라 적절한 수준의 개인정보 보호를 제공하는 것으로 인정하는 EEA 외부의 모든 국가를 의미합니다.
- (e) "컨트롤러를 대신하는 데이터 처리"는 컨트롤러를 대신하여 수행되는 개인 데이터의 처리를 의미하며 GDPR 의 Article 28 에 따라 해석됩니다.
- (f) "MBAG"는 Mercedes-Benz AG, Mercedesstraße 120, 70372 Stuttgart, Germany 를 의미합니다.
- (g) "MBK"는 Mercedes-Benz Korea Ltd., 416, Hangang-daero, Jung-gu, Seoul, Republic of Korea 를 의미합니다.
- (h) "조항"은 총칭하여 통제자를 대신하는 데이터 처리에 관한 조항과 컨트롤러 간 조항을 의미합니다.

- (i) "컨트롤러를 대신하는 데이터 처리에 관한 조항"은 파트 B 에 명시된 조항을 의미합니다.
- (j) "공동 관리자 조항"은 파트 A 에 명시된 조항을 의미합니다. 공동 관리자 조항은 MBK 와 ASP 간의 개인 데이터 전송 및 사용에 적용되며, 당사자는 관련 데이터 보호법에 따라 각 당사자에 대해 제공되는 경우 각각 공동 관리자 역할을 합니다.
- (k) "GDPR"은 2016 년 4 월 27 일 유럽 의회 및 이사회의 규정(EU) 2016/679 를 의미하며, 개인 데이터 처리와 관련된 자연인 보호 및 해당 데이터의 자유로운 이동에 관한 규정 및 지침 95/46/EC(일반 데이터 보호 규정)를 폐지합니다.
- (l) "공동 관리자"는 이러한 처리의 목적이 둘 이상의 관리자 간에 공동으로 결정되고 GDPR 의 26 항에 따라 해석되는 개인 데이터 처리를 의미합니다.
- (m) "회원국"은 EU 회원국인 국가를 의미합니다.
- (n) "서비스"는 관련 별도 계약 및 본 계약의 일부에 자세히 설명된 애프터세일즈 관련 서비스를 의미합니다 .

1.2 본 계약에서:

- (a) 법률 조항에 대한 언급에는 해당 조항에 따라 수시로 제정되는 하위 법률이 포함됩니다.
- (b) 본 계약에 대한 참조에는 부록 및 부록이 포함됩니다.
- (c) 본 계약을 해석할 때 표제는 무시되어야 합니다. 그리고
- (d) 본 계약에 상충 또는 불일치가 있는 경우 상충 또는 불일치는 우선하는 조항에 의해 해결됩니다.

2. 범위

2.1 본 조항 은 파트 A 및 B 의 부록에 추가로 정의된 대로 처리되는 관련 개인 데이터와 관련하여 컨트롤러(또는 해당 당사자에 대한 해당 데이터 보호법에 따라 그러한 개념이 존재하는 경우 공동 컨트롤러) 또는 프로세서로서의 역할을 수행하는 당사자 간에 적용됩니다.

2.2 본 계약을 이행할 때 각 당사자는 상대방 당사자에게 구속력이 있는 현지 데이터 보호법의 세부 사항을 존중하는 취급을 준수합니다.

이를 감안할 때, 각 당사자는 관련 데이터 보호법에 따라 컨트롤러 또는 공동 컨트롤러로 간주될 수 있는지 여부를 정의해야 하며, 보다 정확하게는 이 특정 상황에서 해당 당사자에게 적용되는 법률을 정의해야 합니다. 해당 법률이 공동 관리자의 개념을 규정하지 않는 경우,

관련 당사자는 본 계약에 따라 관리자로 간주되며, 다른 당사자는 해당되는 경우 공동 관리자로 간주될 수 있습니다. 결과적으로, 당사자 중 한 당사자가 관련 데이터 보호법의 의미에서 공동 컨트롤러로 간주되는 반면 다른 당사자는 그렇지 않은 경우, 본 계약의 조항은 각 당사자에게 동일하게 적용되는 관련 데이터 보호법에 따른 각 의무를 충족하기 위한 것입니다. 그러나 전술한 내용은 본 계약의 적용 가능성 및 각 당사자에 대한 계약으로 인한 의무를 제한하거나 영향을 미치지 않습니다.

2.3 각 당사자는 관리자 또는 처리자로서 하위 처리자(있는 경우)에게 최소한 유사한 수준의 보호를 제공할 의무를 부과하며, 하위 처리자와 적절한 계약을 체결하기 전에 하위 처리자가 MBK의 보안 및 개인정보 보호 지침과 요구 사항을 충족하도록 합니다.

3. 수정 및 변형

양 당사자는 기본 계약(Use_ASP_B2B 연결 약관)에서 합의된 메커니즘에 따라 본 계약을 업데이트하거나 보완할 수 있습니다.

4. 기간 및 종료

4.1 본 계약은 양 당사자가 본 약관을 전자적으로(각 약관의 일부로) 수락함으로써 체결하는 시점부터 효력이 발생합니다. 본 계약의 각 당사자는 해당 당사자가 계약을 정당하게 체결한 날부터 계약에 포함된 조건에 구속됩니다.

4.2 본 계약은 당사자 간의 계약 관계(본 계약의 일부)가 종료되거나 서비스 제공이 중단되는 한 유효하며, 향후 어느 사건이 발생하는지에 따라 본 계약에 따른 당사자의 의무는 한 당사자의 개인 데이터가 다른 당사자에 의해 처리되는 한 계속됩니다.

5. 통지

본 계약에 따라 제공되는 모든 통지(이하 "통지")는 텍스트 형식이어야 합니다.

6. 속제

ASP는 MBK의 사전 서면 동의 없이 본 계약에 따른 권리 또는 의무를 양도하거나 이전할 수 없습니다.

7. 책임

당사자는 본 계약에 따른 의무 위반 및/또는 관련 데이터 보호법의 기타 위반으로 인해 발생하는 제 3자의 청구 또는 기타 손실 또는 손해(특히 각자의 영향권 내에서 발생한 손해)에 대해 서로에게 책임을 집니다. 상대방이 그러한 의무를 인지하지 못한 경우, 당사자 중 일방이 관련 데이터 보호법에 따라 데이터 주체가 입은 손해에 대해 전액을 배상할 의무가 있고

그렇게 한 경우, 해당 당사자는 상대방 당사자로부터 손해에 대한 상대방의 책임 분담에 해당하는 보상 부분을 회수할 수 있습니다.

8. 분리

8.1 본 계약의 조항이 전체 또는 부분적으로 불법, 무효 또는 시행 불가능한 것으로 판명되는 경우, 본 계약의 나머지 조항의 적법성, 유효성 및 시행 가능성은 영향을 받지 않습니다.

8.2 당사자들은 무효 조항으로 당사자들이 추구하는 경제적 목표에 가능한 한 근접한 효력을 갖는 무효 조항을 보완하는 데 동의합니다. 위의 조항은 계약이 불완전한 경우 “타 계약 조항의 준용 (mutatis mutandis)”를 적용합니다.

9. 준거법 및 관할권

공연 장소는 대한민국이며, 관할권 및 재판지는 서울중앙지방법원 관할법원에 있습니다. 국제사법 규정을 제외하고는 대한민국의 법률이 적용됩니다. 양 당사자는 1980년 4월 11일 국제 물품 매매 계약에 관한 유엔 협약(UN Convention on Contracts for the International Sale of Goods)에 기초한 통일 국제연합(UN) 판매법의 적용을 배제하는 데 동의합니다.

10. 개별 계약과의 관계

10.1 본 계약은 본 계약에서 명시적으로 규정된 데이터 처리 활동과 관련하여 당사자 간에 이전에 존재했던 모든 데이터 보호 규정을 대체합니다.

10.2 명시된 목적을 위해 각 서비스를 제공 또는 사용하거나 해당 데이터를 전송할 때 당사자의 책임을 포함하여 여기에 명시적으로 언급되지 않은 모든 문제는 당사자 간의 추가 기존 계약(섹션 4.2에 명시된 계약 관계에서 파생됨)의 조건에 의해 규율됩니다.

10.3 본 계약의 조건과 10.2항에 언급된 다른 계약 사이에 불일치가 있는 경우 본 계약의 조건이 우선합니다.

파트 A

JOINT-CONTROLLER 조항

서문

B2B Connect 영역에서의 비즈니스 협력 맥락에서 당사자는 특정 비즈니스 목적을 위해 개인 데이터를 공유하고 데이터 보호법의 의미 내에서 데이터 컨트롤러로서 처리하기를 원합니다(이하 "협력"이라고 함).

본 조항(이하 "계약"이라고 함)에서 당사자는 협력의 맥락에서 수행되는 개인 데이터 처리와 관련된 당사자의 권리와 의무 및 관련 데이터 보호 의무 준수와 관련된 각각의 책임을 명시합니다.

이러한 배경에서 당사자들은 다음과 같은 계약을 체결합니다.

1. 계약의 목적

본 계약은 공동 관리자로서 개인 데이터를 처리할 때 당사자(이하 "관리자")의 권리와 의무를 규율합니다.

2. 공동 통제하에 처리되는 범위

2.1 협력 전반에 걸쳐 당사자는 GDPR 26항의 의미 내에서 공동 컨트롤러로서 개인 데이터를 처리합니다. 본 계약의 조항은 관리자의 직원 또는 관리자가 위탁한 처리자가 관리자를 대신하여 개인 데이터를 처리하는 공동 관리자 직분에 따라 수행되는 모든 처리 활동에 적용됩니다. 각각의 역할, 책임 및 역량을 포함한 공동 관리자로서의 처리 범위와 처리에 대한 자세한 내용은 부록 1에 명시되어 있습니다.

2.2 부록 1의 정보는 참조가 이루어지는 병렬로 제공된 정보 텍스트를 포함하여 당사자가 병렬로 체결한 계약(예: 서비스 계약)의 프로세스 및 활동 설명에 의해 입증됩니다.

3. 관리자의 의무

3.1 관리자는 관련 데이터 보호법의 관련 조항에 따라 개인 데이터 처리를 수행하며, 본 계약에서 다루는 처리 활동 및 본 계약에 명시된 처리 활동과 관련하여 공동 컨트롤러와 관련된 GDPR 조항을 준수할 책임이 있습니다. 특히, 부록 1에 설명된 처리 작업 및 목적에 필요한 개인 데이터만 수집되도록 해야 합니다. 또한 관리자는 데이터 최소화 원칙을 준수해야 합니다(참조). GDPR 5 (1) (c)항).

3.2 각 관리자는 아래 및 부록 1에 할당된 작업 및 책임 범위 내에서 개인 데이터 수집 및 처리의 적법성에 대해 내부적으로 책임을 집니다.

3.3 관리자는 협력의 맥락에서 개인 데이터 처리에 관련된 모든 사람이 해당 데이터에 액세스하기 전에 기밀 유지 및 데이터 비밀 유지 의무를 준수하거나 준수하도록 해야 하며, 이는 활동 중 및 활동 종료 후에도 효력이 발생합니다. 그들은 관련자가 자신과 관련된 데이터 보호 조항에 대해 교육을 받았는지 확인해야 합니다.

3.4 관리자는 구조화되고 일반적으로 사용되며 기계가 읽을 수 있는 형식으로 개인 데이터를 저장해야 합니다. 개인 데이터는 정확해야 하며 필요한 경우 최신 상태로 유지되어야 합니다. 관리자는 이를 구현하기 위해 모든 조치를 취해야 합니다.

3.5 관리자는 처리 활동을 검토하는 동안 데이터 보호 조항과 관련된 오류나 불규칙성을 발견하는 경우 즉시 서로에게 완전히 알려야 합니다.

3.6 적절한 처리의 증거가 되는 문서(cf. 제5조 (2) GDPR)은 각 당사자가 계약 종료 이후에도 법적 권한 및 의무에 따라 보관해야 합니다.

4. 기술적, 조직적 조치

4.1 최첨단 기술, 구현 비용, 처리의 성격, 범위, 컨텍스트 및 목적뿐만 아니라 자연인의 권리와 자유에 대한 위험의 다양한 가능성과 심각성을 고려하여 관리자는 위험에 적합한 보안 수준을 보장하기 위해 적절한 기술 및 조직적 조치를 구현해야 합니다. 적절한 경우 다음을 포함합니다.

- 지속적으로 처리와 관련된 시스템 및 서비스의 기밀성, 무결성, 가용성 및 복원력을 보장할 수 있는 능력;
- 물리적 또는 기술적 사고 발생 시 개인 데이터의 가용성 및 액세스를 신속하게 복원할 수 있는 능력;
- 처리의 보안을 보장하기 위해 기술적 및 조직적 조치의 효과를 주기적으로 검토, 평가 및 평가하는 절차; 그리고
- 기술 및 데이터 보호 친화적인 기본 설정을 통해 데이터 보호 원칙을 적절하게 준수하기 위한 절차(참조. Art. 25 GDPR)를 참조하십시오.

관리자는 추가 요구 사항을 별도로 지정할 수 있습니다.

4.2 관리자는 특히 GDPR 12 – 22항에 따라 데이터 주체의 권리가 항상 법적 요구 사항에 따라 행사될 수 있도록 필요한 모든 기술적 및 조직적 조치를 취해야 합니다. 필요한 경우, 통제관은 조치의 구체적인 설계에 동의하고 그 이행을 공동으로 결정해야 합니다.

4.3 시스템의 구현, 기본 설정 및 운영은 관련 데이터 보호법의 요구 사항, 특히 설계에 의한 개인 정보 보호 및 기본적으로 개인 정보 보호 원칙에 따라 수행되어야 하며 최신 기술에 따라 적절한 기술 및 조직적 조치를 사용해야 합니다.

5. 데이터 보호법 및 데이터 주체의 권리 준수에 대한 책임

- 5.1 데이터 주체는 GDPR 12 – 22항에 따라 모든 컨트롤러에 대해 자격이 있는 데이터 주체 권리를 주장할 수 있으며, 원칙적으로 외부 관계에서 해당 권리의 이행에 대한 책임은 유지됩니다.
- 5.2 부록 1 또는 다른 맥락에서 달리 규정되지 않는 한, 추가 처리를 위해 다른 컨트롤러에게 전송하기 전에 데이터 주체로부터 해당 개인 데이터를 원래 수집한 컨트롤러 또는 데이터 주체와 직접적인 계약 관계를 맺었거나 맺고 있는 컨트롤러는 데이터 주체의 중심 연락 창구로 남아 GDPR의 적용을 받는 컨트롤러가 다음 이행에 관한 책임을 지도록 지원해야 합니다 내부 관계에서 Art. 12 – 22 GDPR에 따른 데이터 주체의 권리. 이러한 지원은 다른 컨트롤러가 해당 권리를 완전히 이행할 수 있도록 하는 방식으로 제공되어야 합니다.
- 5.3 관리자는 데이터 주체 권리를 이행하는 데 있어 적절한 범위까지 서로를 지원하고, 해당 요청에 대해 서로에게 알리고, 적시에 필요한 모든 정보를 서로에게 제공합니다. 개인 데이터가 삭제되는 경우 당사자는 사전에 서로에게 알려야 합니다. 상대방은 정당한 이유(예: 데이터를 보존할 법적 의무가 있는 경우)로 삭제에 반대할 수 있습니다.
- 5.4 데이터 주체는 GDPR 13항 및 14항에 따라 처리에 대한 정보를 제공받아야 합니다. 관리자는 정보 의무를 이행하는 데 있어 서로를 지원하고 관련 데이터 처리 활동에 필요한 정보를 서로에게 제공해야 합니다.
- 5.5 부록 1 또는 다른 맥락에서 달리 규정되지 않는 한, 추가 처리를 위해 다른 컨트롤러에게 전송하기 전에 데이터 주체로부터 해당 개인 데이터를 원래 수집했거나 데이터 주체와 직접적인 계약 관계를 맺었거나 맺고 있는 컨트롤러는 데이터 주체에게 본 규정의 주요 내용에 대한 정보를 제공할 책임이 있습니다. 이를 위해 관리자는 요청 시 데이터 주체에게 본 섹션 6의 조항을 제공할 수 있습니다.
- 5.6 각 관리자는 감독 기관 및 개인 데이터 침해의 영향을 받는 데이터 주체에 대한 잠재적인 데이터 침해로 인한 보고 및 통지 의무에 대해 각자의 책임 영역에 대한 책임이 있습니다(참조. GDPR 33, 34항). 본 계약이 적용되는 처리 활동과 관련하여 보고 가능한 사건이 발생한 경우, 관리자는 감독 기관에 사건을 보고하거나 데이터 주체에게 알리기 전에 지체 없이 서로에게 알려야 합니다. 관리자는 사실을 명확히 하고 데이터 주체를 보호하기 위한 적절한 조치를 취하는 데 최선을 다해 서로를 지원해야 합니다. 취해야 할 조치의 필요성, 내용 및 범위에 대한 결정은 통지할 의무가 있는 각 관리자가 내립니다.
- 5.7 당사자들은 필요에 따라 요청 시 데이터 보호 영향 평가를 준비하는 데 있어 서로를 지원해야 합니다(참조. GDPR 35항) 또는 당국의 협의(참조. GDPR 36항)를 참조하십시오. 당사자들은 적절한 시기에 각자의 활동 영역에서 이를 위해 필요한 정보를 서로에게 제공해야 합니다.
- 5.8 각 관리자는 자신의 책임에 따라 처리 활동에 대한 기록을 유지해야 합니다. 관리자는 처리 활동에 대한 적절한 기록을 유지하는 데 필요한 정보를 서로에게 제공해야 합니다.

5.9 적절한 데이터 처리의 증거 역할을 하는 문서(참조. 섹션 5.6)는 계약 관계가 종료된 후에도 각 당사자가 보관해야 합니다. 관리자는 관련 개인 데이터를 보유하기 위한 기존의 모든 법적 의무를 준수하는지 확인해야 합니다.

5.10 달리 합의되지 않는 한, 각 관리자는 본 계약에 따른 의무를 이행하는 데 발생하는 비용(있는 경우)을 부담해야 하며, 해당 의무 이행에 대해 다른 관리자에게 보수를 청구할 수 없습니다.

6. 프로세서

6.1 각 컨트롤러는 프로세서를 사용할 수 있습니다.

6.2 컨트롤러가 본 계약의 적용을 받는 처리 활동을 위해 처리자를 고용하는 경우, 이는 해당 데이터 보호법에 따른 요구 사항이 충족되는 범위 내에서만 수행됩니다.

6.3 관리자는 요청 시 본 계약에 따라 데이터 처리 활동에 관련된 처리자 목록을 서로에게 제공해야 합니다. 관리자는 요청 시 다른 프로세서의 추가 또는 교체와 관련하여 의도된 변경 사항을 다른 관리자에게 알려야 합니다.

6.4 이는 관리자가 보조 서비스를 위해 제3자에게 위탁하는 경우에는 적용되지 않습니다. 여기에는 우편, 통신, 배송 및 수령 서비스, 시설 관리 서비스가 포함되지만 이에 국한되지 않습니다. 관리자는 해당 법적 요구 사항에 따라 각 서비스 제공업체와 적절한 계약 및 의무를 이행하고 개인 데이터 보안과 관련하여 적절한 통제 조치를 제공할 의무가 있습니다.

7. 유럽경제지역(EEA) 안팎에서의 처리

7.1 원칙적으로 처리는 유럽 연합 회원국, 유럽 경제 지역(EEA) 국가 또는 적절한 수준의 보호를 제공하는 국가에서 이루어집니다. EEA 이외의 다른 국가에서의 처리 활동은 개인 데이터의 국제 전송에 대한 해당 조항을 준수하는 경우 허용됩니다.

7.3 Art. 44 이하 참조 GDPR의 의미 내에서 제3국으로의 개인 데이터 전송에 대한 보장이 없는 경우, Art. 47 GDPR에 따른 구속력 있는 기업 규칙과 같은 EU 표준 계약 조항의 조항이 적용됩니다.

8. 책임

8.1 관리자는 법률 조항에 따라 데이터 주체에 대해 책임을 집니다.

8.2 관리자는 책임을 발생시킨 원인에 대한 책임의 일부를 부담하는 한 내부 관계에서 책임을 집니다. 이는 데이터 보호 조항 위반으로 관리자에게 부과된 벌금과 관련해서도 적용되며, 벌금의 대상이 되는 관리자는 먼저 공식 결정에 대한 모든 법적 구제책을 소진해야 합니다. 컨트롤러가 위반에 대한 내부 책임 분담에 해당하지 않는 벌금을 계속 부과받는 경우, 각각의 다른 컨트롤러는 벌금에 의해 승인된 위반에 대한 책임을 지는 범위 내에서 해당 컨트롤러에게 벌금을 면제할 의무가 있습니다.

8.3 관련 서비스에 대한 추가 계약에서 합의된 책임 제한은 그에 따라 적용됩니다.

9. 위임장 (Power of Attorney)

9.1 MBK 는 MBAG 의 명의로 그리고 그 부속서 절반에 따라 이러한 공동 관리자 조항(부속서 포함)을 실행할 수 있는 권한을 부여받았으며, 따라서 MBAG 를 부속서 1 에 명시된 역할을 가진 다른 컨트롤러로서 이러한 공동 관리자 조항의 당사자로 만들 수 있습니다. MBAG 가 아래 부록 1(또는 부록 2)에 컨트롤러로 표시되지 않은 경우, MBAG 는 이와 관련하여 본 계약의 당사자가 되지 않습니다. ASP 는 MBAG 가 부속서를 포함하여 본 파트 A(본 계약에 달리 명시되지 않는 한 계약의 다른 부분 제외)에 따라 컨트롤러로서의 모든 권리와 의무를 부여받고 이에 따라 당사자가 되는 것을 확인하고 동의합니다.

9.2 MBK 는 회사명, 주소, 계약 내용 등 각 계약 관계가 성립된 ASP 에 대해 MBAG 에 알리고, MBAG 의 요청이 있을 경우 체결된 계약서 및 특히 본 파트 A 의 사본을 제공하는 등 충분한 증거를 제공할 수 있습니다.

부록 1: 공동 작업의 역할, 작업 및 범위

1. Business Analytics 관련 처리 활동

| 절차 | 목적/범위 | 역할 및 작업 | 데이터 범주 및 데이터 주체 |
|-----------------------|--|---|---|
| 셀러 센터의 ISP 에 대한 티켓 지원 | ASP 에 판매자 센터의 티켓 및 계정 개설 요청을 통해 ISP 를 지원하는 옵션을 제공합니다. | <p>MBK: 컨트롤러</p> <p>ASP 가 셀러 센터에서 티켓으로 ISP 를 지원할 수 있는 옵션을 제공하고 ISP 에 통지하면 ASP 에서 티켓 및 요청 정보를 사용할 수 있도록 합니다. 항공권 정보의 기술적 처리를 담당합니다.</p> <p>ASP: 컨트롤러</p> <p>ISP 와 협력하여 ISP 에 대한 티켓/요청을 지원합니다. 제공된 정보를 적절하게 취급하고 올바르게 처리할 책임이 있습니다.</p> | <p>ISP 데이터: ISP 회사명, 사용자 이름, 사용자 ID, 주소, 이메일, 전화, 티켓 또는 요청 내용(날짜, 제목)</p> <p>ASP 데이터: 회사명, 사용자명, 아이디, 주소, 이메일, 전화번호</p> |
| 비즈니스 분석 | <p>B2B Connect 플랫폼 운영을 통해 획득한 매출 데이터는 비즈니스 운영을 분석하고 집계된 보고서를 MBAG, MBK 및 ASP 에 제공하는 데 사용됩니다.</p> <p>보고서는 일반적으로 자동화된 계산(애플리케이션 기반)에 의해 생성됩니다.</p> <p>예외적인 경우 데이터는 추가 분석을 실행하기 위해 다른 소스(예: 다른 MBAG 부서의 다른 데이터베이스)의 데이터와 병합됩니다.</p> <p>MBAG 와 그 직원들은 알아야 할 필요성 원칙에 따라 엄격하게 운영됩니다.</p> | <p>엠바그: 컨트롤러</p> <p>비즈니스 로직을 운영하고 비즈니스 데이터로 데이터베이스를 호스팅하며, 제공된 데이터를 기반으로 집계된 평가/보고서를 작성합니다.</p> <p>MBK: 컨트롤러</p> <p>B2B 플랫폼 거래 관련 데이터를 전송하여 위의 프로세스에 사용할 수 있습니다. 집계된 보고서 수신</p> <p>ASP: 컨트롤러</p> <p>B2B 플랫폼 거래 관련 데이터를 전송하여 위의 프로세스에 사용할 수 있습니다. 집계된 보고서 수신</p> | <p>ISP 데이터: ISP 회사명, 사용자명, 사용자 아이디, 주소, 이메일, 전화번호, 주문내역(주문일자, 주문한 부품/서비스, 주문수량, 판매, 주문미주문(매출 손실), B2B Connect Platform/A/S 관련 서비스 이용 빈도, 배송 시간)</p> <p>ASP 데이터: 회사명, 사용자명, 아이디, 주소, 이메일, 전화번호</p> |

2. 받는 사람

각자의 관리 책임을 수행하기 위해 필요한 경우에만 개인 데이터가 공개되는 전담 역할을 가진 제한된 개인[예: HR, IT 및 재무 계약자(해당되는 경우)을 포함한 계약자] 그룹 법인, 컨설턴트, 감사, 회계사; 금융 기관; 법 집행 기관, 정부 기관, 규제 당국.

부록 2: EU 표준 계약 조항

표준 계약 조항

섹션 1

조항 1

목적 및 범위

- (a) 이러한 표준 계약 조항의 목적은 개인 데이터 처리와 관련된 자연인 보호 및 개인 데이터를 제 3 국으로 전송하기 위한 해당 데이터의 자유로운 이동에 관한 2016 년 4 월 27 일 유럽 의회 및 이사회 의 규정(EU) 2016/679 의 요구 사항을 준수하는 것입니다.
- (b) 당사자들:
- () 부록 I.A 에 나열된 대로 개인 데이터를 전송하는 자연인 또는 법인, 공공 기관, 에이전시 또는 기타 단체(이하 "법인")(이하 "데이터 수출자")
 - (i) 부록 I.A 에 나열된 바와 같이 본 조항의 당사자이기도 한 다른 법인을 통해 직접 또는 간접적으로 데이터 수출업자로부터 개인 데이터를 받는 제 3 국의 법인(이하 각 "데이터 수입업자")

이러한 표준 계약 조항(이하 : "조항").

- (c) 이 조항은 부록 I.B.에 명시된 개인 데이터의 전송과 관련하여 적용됩니다.
- (d) 여기에 언급된 부록을 포함하는 이 조항의 부록은 이 조항의 필수적인 부분을 형성합니다.

제2 항

조항의 효력 및 불변성

- (a) 본 조항은 규정(EU) 2016/679 의 46(1)조 및 46(2)(c)조에 따라 집행 가능한 데이터 주체 권리 및 효과적인 법적 구제책을 포함한 적절한 보호 조치를 규정하며, 컨트롤러에서 프로세서로의 데이터 전송과 관련하여 규정(EU) 2016/679 의 28(7)조에 따른 표준 계약 조항을 명시합니다. 단, 적절한 모듈을 선택하거나 부록의 정보를 추가 또는 업데이트하는 경우를 제외하고는 수정되지 않습니다. 이는 당사자들이 본 조항에 명시된 표준 계약 조항을 더 넓은 계약에 포함시키거나 다른 조항 또는 추가 보호 장치를 추가하는 것을 막지 않습니다(단, 본 조항과 직간접적으로 모순되거나 데이터 주체의 기본권 또는 자유를 침해하지 않는 한).
- (b) 이러한 조항은 Regulation (EU) 2016/679 에 따라 데이터 수출자에게 적용되는 의무를 침해하지 않습니다.

제3 항

제3 자 수혜자

(a) 데이터 주체는 제 3 자 수혜자로서 데이터 수출업자 및/또는 데이터 수입업자에 대해 이러한 조항을 적용하고 시행할 수 있으며, 다음과 같은 예외가 있습니다.

(ii) 제 1 항, 제 2 항, 제 3 항, 제 6 항, 제 7 항;

(iii) 8.5(e)항 및 8.9(b)항

(iv) 조항 12(a) 및 (d);

(v) 조항 13;

(vi) 조항 15.1(c), (d) 및 (e);

(vii) 조항 16(e);

(viii) 조항 18(a) 및 (b).

(b) 단락 (a)는 규정(EU) 2016/679 에 따른 데이터 주체의 권리를 침해하지 않습니다.

제 4 항

해석

(a) 본 조항이 규정(EU) 2016/679 에 정의된 용어를 사용하는 경우, 해당 용어는 해당 규정과 동일한 의미를 갖습니다.

(b) 이 조항은 규정(EU) 2016/679 의 조항에 비추어 읽고 해석해야 합니다.

(c) 본 조항은 규정(EU) 2016/679 에 규정된 권리 및 의무와 상충되는 방식으로 해석되어서는 안 됩니다.

제 5 항

계층

본 조항과 당사자 간의 관련 계약 조항 사이에 모순이 있는 경우, 본 조항이 합의되거나 그 이후에 체결되는 시점에 존재하는 경우 본 조항이 우선합니다.

제 6 항

전송에 대한 설명

전송에 대한 세부 정보, 특히 전송되는 개인 데이터의 범주 및 전송 목적은 부록 I.B.에 명시되어 있습니다.

제 7 항

도킹 조항

(a) 본 조항의 당사자가 아닌 법인은 당사자의 동의 하에 데이터 수출업자 또는 데이터 수입업자로서 부록을 작성하고 부록 I.A.에 서명하여 언제든지 본 조항에 동의할 수 있습니다.

- (b) 부록을 완성하고 부록 I.A.에 서명하면 가입 주체는 본 조항의 당사자가 되며 부록 I.A.의 지정에 따라 데이터 수출업자 또는 데이터 수입업자의 권리와 의무를 갖습니다.
- (c) 가입 법인은 당사자가 되기 전의 기간부터 본 조항에 따라 발생하는 어떠한 권리나 의무도 갖지 않습니다.

섹션 II – 당사자의 의무

제8 항

데이터 보호 보호 장치

데이터 수출자는 적절한 기술적 및 조직적 조치의 구현을 통해 데이터 수입자가 본 조항에 따른 의무를 이행할 수 있는지 확인하기 위해 합당한 노력을 기울였음을 보증합니다.

8.1 목적 제한

데이터 수입자는 부록 I.B.에 명시된 대로 전송의 특정 목적을 위해서만 개인 데이터를 처리해야 합니다. 다음과 같은 다른 목적으로만 개인 데이터를 처리할 수 있습니다.

- (ix) 정보주체의 사전 동의를 얻은 경우
- (x) 특정 행정, 규제 또는 사법 절차의 맥락에서 법적 청구의 설정, 행사 또는 방어를 위해 필요한 경우; 또는
- (xi) (데이터 주체 또는 다른 자연인의 중요한 이익을 보호하기 위해 필요한 경우.

8.2 투명성

(a) 데이터 주체가 10 항에 따라 자신의 권리를 효과적으로 행사할 수 있도록 데이터 수입자는 직접 또는 데이터 수출자를 통해 데이터 주체에게 다음 사항을 알려야 합니다.

- (xii) 신원 및 연락처 세부 정보;
- (xiii) 처리되는 개인 데이터의 범주
- (xiv) 이 조항의 사본을 얻을 수 있는 권리;
- (xv) 개인 데이터를 제 3 자, 수신자 또는 수신자 범주(의미 있는 정보를 제공하기 위해 적절한 경우)에게 전송하려는 경우, 그러한 제 3 자 전송의 목적 및 8.7 항에 따른 근거.

(b) (a)항은 데이터 수출업자가 해당 정보를 이미 제공했거나 정보 제공이 불가능하거나 데이터 수입업자에게 과도한 노력을 수반하는 경우를 포함하여 데이터 주체가 이미 정보를 보유하고 있는 경우에는 적용되지 않습니다. 후자의 경우 데이터 수입자는 가능한 한 정보를 공개적으로 사용할 수 있도록 해야 합니다.

(c) 요청 시 당사자는 자신이 작성한 부록을 포함하여 본 조항의 사본을 데이터 주체가 무료로 사용할 수 있도록 해야 합니다. 비즈니스 비밀 또는 개인 데이터를 포함한 기타 기밀 정보를 보호하는 데 필요한 범위 내에서 당사자는 사본을 공유하기 전에 부록 텍스트의 일부를 수정할 수 있지만, 데이터 주체가 그 내용을 이해하거나 권리를 행사할 수 없는 경우 의미 있는 요약물을 제공해야 합니다. 요청 시 당사자는 편집된 정보를 공개하지 않고 가능한 한 데이터 주체에게 수정 이유를 제공해야 합니다.

- (d) 단락 (a)에서 (c)는 규정(EU) 2016/679 의 13 조 및 14 조에 따른 데이터 수출자의 의무를 침해하지 않습니다.

8.3 정확성 및 데이터 최소화

- (a) 각 당사자는 개인 데이터가 정확하고 필요한 경우 최신 상태로 유지되도록 해야 합니다. 데이터 수입자는 처리 목적과 관련하여 부정확한 개인 데이터가 지체 없이 삭제 또는 수정되도록 모든 합리적인 조치를 취해야 합니다.
- (b) 당사자 중 한 명이 전송 또는 수신한 개인 데이터가 부정확하거나 오래된 것임을 알게 된 경우 지체 없이 다른 당사자에게 알려야 합니다.
- (c) 데이터 수입자는 개인 데이터가 적절하고 관련성이 있으며 처리 목적과 관련하여 필요한 것으로 제한되도록 해야 합니다.

8.4 스토리지 제한

데이터 수입자는 개인 데이터를 처리 목적에 필요한 기간 이상으로 보관해서는 안 됩니다. 이 의무를 준수하기 위해 적절한 기술적 또는 조직적 조치를 취해야 하며, 여기에는 보존 기간 종료 시 데이터 및 모든 백업의 삭제 또는 익명화가 포함됩니다.

8.5 처리의 보안

- (a) 데이터 수입업자 및 전송 중에 데이터 수출업자는 우발적 또는 불법적 파기, 손실, 변경, 무단 공개 또는 액세스(이하 "개인 데이터 침해")로 이어지는 보안 위반에 대한 보호를 포함하여 개인 데이터의 보안을 보장하기 위해 적절한 기술적 및 조직적 조치를 구현해야 합니다. 적절한 보안 수준을 평가할 때 최첨단 기술, 구현 비용, 처리의 성격, 범위, 컨텍스트 및 목적, 데이터 주체의 처리와 관련된 위험을 충분히 고려해야 합니다. 당사자들은 특히 암호화 또는 가명화에 의존하는 것을 고려해야 하며, 전송 중을 포함하여 처리 목적이 그러한 방식으로 충족될 수 있는 경우에 이를 고려해야 합니다.
- (b) 당사국들은 부속서 II 에 규정된 기술적, 조직적 조치에 합의하였다. 데이터 수입자는 이러한 조치가 적절한 수준의 보안을 계속 제공하는지 확인하기 위해 정기적인 점검을 수행해야 합니다.
- (c) 데이터 수입자는 개인 데이터를 처리할 권한이 있는 사람이 기밀 유지를 약속했거나 적절한 법적 기밀 유지 의무가 있는지 확인해야 합니다.
- (d) 본 조항에 따라 데이터 수입업자가 처리하는 개인 데이터와 관련하여 개인 데이터 침해가 발생하는 경우, 데이터 수입업자는 발생할 수 있는 부작용을 완화하기 위한 조치를 포함하여 개인 데이터 침해를 해결하기 위한 적절한 조치를 취해야 합니다.
- (e) 자연인의 권리와 자유에 위협을 초래할 수 있는 개인 데이터 침해의 경우, 데이터 수입자는 제 13 항에 따라 데이터 수출자와 관할 감독 기관에 지체 없이 통지해야 합니다. 이러한

통지에는 i) 위반의 성격에 대한 설명(가능한 경우 관련 데이터 주체 및 개인 데이터 기록의 범주 및 대략적인 수 포함), ii) 발생할 수 있는 결과, iii) 위반을 해결하기 위해 취하거나 제안된 조치, iv) 추가 정보를 얻을 수 있는 연락처의 세부 정보가 포함되어야 합니다. 데이터 수입자가 모든 정보를 동시에 제공할 수 없는 경우, 과도한 추가 지연 없이 단계적으로 제공할 수 있습니다.

- (f) 자연인의 권리와 자유에 높은 위험을 초래할 수 있는 개인 데이터 침해의 경우, 데이터 수입자는 필요한 경우 데이터 수출자와 협력하여 (e)항에 언급된 정보와 함께 관련 데이터 주체에게 개인 데이터 침해 및 그 성격을 해당 데이터 주체에게 부당한 지체 없이 통지해야 합니다. ii)부터 iv)까지), 데이터 수입자가 자연인의 권리 또는 자유에 대한 위험을 크게 줄이기 위한 조치를 구현하지 않았거나 통지에 과도한 노력이 수반되지 않는 한. 후자의 경우, 데이터 수입자는 대신 공개 커뮤니케이션을 발행하거나 유사한 조치를 취하여 개인 데이터 침해를 대중에게 알려야 합니다.
- (g) 데이터 수입자는 개인 데이터 침해와 관련된 모든 관련 사실(영향 및 취한 시정 조치 포함)을 문서화하고 이에 대한 기록을 보관해야 합니다.

8.6 민감한 데이터

전송에 인종 또는 민족, 정치적 견해, 종교적 또는 철학적 신념 또는 노동 조합 가입 여부를 드러내는 개인 데이터, 자연인을 고유하게 식별하기 위한 유전자 데이터 또는 생체 인식 데이터, 건강 또는 개인의 성생활 또는 성적 취향에 관한 데이터, 또는 범죄 유죄 판결 또는 범죄와 관련된 데이터(이하 "민감한 데이터")가 포함되는 경우 데이터 수입자는 데이터의 특정 특성과 관련된 위험에 맞게 조정된 특정 제한 및/또는 추가 보호 조치를 적용해야 합니다. 여기에는 개인 데이터에 액세스할 수 있는 직원 제한, 추가 보안 조치(예: 가명화) 및/또는 추가 공개와 관련된 추가 제한이 포함될 수 있습니다.

8.7 제 3 자 환승

데이터 수입자는 제 3 자가 해당 모듈에 따라 본 조항에 구속되거나 이에 동의하지 않는 한 유럽 연합 외부에 위치한 제 3 자(데이터 수입자와 동일한 국가 또는 다른 제 3 국, 이하 "제 3 자 전송")에 개인 데이터를 공개해서는 안 됩니다. 그렇지 않은 경우, 데이터 수입자에 의한 제 3 자 전송은 다음과 같은 경우에만 발생할 수 있습니다.

- (xvi) 제 45 조 규정(EU) 2016/679 에 의거하여 적정성 결정의 혜택을 받는 국가에게 적용됩니다.
- (xvii) 그렇지 않으면 제 3 자는 해당 처리와 관련하여 규정 (EU) 2016/679 의 46 조 또는 47 조에 따라 적절한 보호 조치를 보장합니다.
- (xviii) 제 3 자는 본 조항에 따른 것과 동일한 수준의 데이터 보호를 보장하는 데이터 수입업자와 구속력 있는 문서를 체결하고, 데이터 수입업자는 이러한 보호 조치의 사본을 데이터 수출업자에게 제공합니다.

- (xix) 특정 행정, 규제 또는 사법 절차의 맥락에서 법적 청구의 설정, 행사 또는 방어에 필요합니다.
- (xx) 데이터 주체 또는 다른 자연인의 중요한 이익을 보호하기 위해 필요한 경우 또는
- (xxi) 다른 조건이 적용되지 않는 경우, 데이터 수입자는 데이터 주체에게 목적, 수신자의 신원 및 적절한 데이터 보호 장치의 부재로 인해 전송될 경우 발생할 수 있는 위험을 알린 후 특정 상황에서 데이터 주체의 향후 전송에 대한 명시적인 동의를 얻은 것입니다. 이 경우 데이터 수입자는 데이터 수출업자에게 이를 알리고 데이터 수출업자의 요청에 따라 데이터 주체에게 제공된 정보의 사본을 데이터 수출업자에게 전송해야 합니다.

모든 제삼자 전송은 데이터 수입자가 본 조항에 따른 다른 모든 보호 장치, 특히 목적 제한을 준수해야 합니다.

8.8 데이터 수입자의 권한에 따른 처리

데이터 수입자는 처리자를 포함하여 자신의 권한 하에 행동하는 모든 사람이 자신의 지시에 따라서만 데이터를 처리하도록 해야 합니다.

8.9 문서화 및 규정 준수

- (a) 각 당사자는 본 조항에 따른 의무 준수를 입증할 수 있어야 합니다. 특히, 데이터 수입자는 자신의 책임 하에 수행된 처리 활동에 대한 적절한 문서를 보관해야 합니다.
- (b) 데이터 수입자는 요청 시 관할 감독 기관에 해당 문서를 제공해야 합니다.

제9 항

(의도적으로 비워 둠)

제10 항

데이터 주체의 권리

- (a) 데이터 수입자는 데이터 수출자의 도움을 받아 데이터 주체의 개인 데이터 처리 및 본 조항에 따른 권리 행사와 관련하여 데이터 주체로부터 받은 모든 문의 및 요청을 지체 없이, 늦어도 문의 또는 요청을 받은 후 1 개월 이내에 처리해야 합니다. 데이터 수입자는 이러한 문의, 요청 및 데이터 주체 권리 행사를 용이하게 하기 위해 적절한 조치를 취해야 합니다. 데이터 주체에게 제공되는 모든 정보는 명확하고 평이한 언어를 사용하여 이해하기 쉽고 쉽게 액세스할 수 있는 형식이어야 합니다.
- (b) 특히, 데이터 주체의 요청이 있을 경우 데이터 수입자는 무료로 다음을 제공합니다.
 - (xxii) 데이터 주체에게 자신에 관한 개인 데이터가 처리되고 있는지 여부를 확인하고, 이 경우 데이터 주체와 관련된 데이터 및 부록 I 의 정보 사본을

제공합니다. 개인 데이터가 전송되었거나 향후 전송될 예정인 경우, 개인 데이터가 전송되었거나 전송될 수신자 또는 수신자 범주(의미 있는 정보를 제공하기 위해 적절한 경우), 그러한 제 3 자 전송의 목적 및 8.7 항에 따른 근거에 대한 정보를 제공합니다. 12(c)(i)항에 따라 감독 당국에 불만을 제기할 권리에 대한 정보를 제공합니다.

(xxiii) 데이터 주체와 관련하여 부정확하거나 불완전한 데이터를 수정합니다.

(xxiv) 해당 데이터가 제 3 자 수혜자 권리를 보장하는 본 조항을 위반하거나 처리된 경우 또는 데이터 주체가 처리의 근거가 되는 동의를 철회하는 경우 데이터 주체에 대한 개인 데이터를 삭제합니다.

(c) 데이터 수입자가 직접 마케팅 목적으로 개인 데이터를 처리하는 경우, 데이터 주체가 이의를 제기하는 경우 해당 목적을 위한 처리를 중단해야 합니다.

(d) 데이터 수입자는 데이터 주체의 명시적인 동의가 있거나 목적지 국가의 법률에 따라 그렇게 할 수 있는 권한이 있는 경우를 제외하고, 데이터 주체와 관련하여 법적 효력을 발생시키거나 이와 유사하게 데이터 주체에게 중대한 영향을 미칠 수 있는 전송된 개인 데이터의 자동화된 처리(이하 "자동화된 결정")만을 기반으로 결정을 내려서는 안 됩니다. 단, 해당 법률이 데이터 주체의 권리와 정당한 이익을 보호하기 위한 적절한 조치를 규정하는 경우. 이 경우 데이터 수입자는 필요한 경우 데이터 수출업자와 협력하여 다음을 수행해야 합니다.

(xxv) 예상되는 자동 결정, 예상되는 결과 및 관련된 논리에 대해 데이터 주체에게 알립니다. 그리고

(xxvi) 적어도 데이터 주체가 결정에 이의를 제기하고, 자신의 관점을 표현하고, 사람의 검토를 받을 수 있도록 함으로써 적절한 보호 장치를 구현합니다.

(e) 데이터 주체의 요청이 과도한 경우, 특히 반복적인 특성으로 인해 데이터 수입자는 요청을 승인하는 데 드는 관리 비용을 고려하여 합리적인 수수료를 부과하거나 요청에 대한 조치를 거부할 수 있습니다.

(f) 데이터 수입자는 대상 국가의 법률에 따라 거부가 허용되고 민주주의 사회에서 규정(EU) 2016/679 의 23(1)항에 나열된 목표 중 하나를 보호하기 위해 필요하고 비례하는 경우 데이터 주체의 요청을 거부할 수 있습니다.

(g) 데이터 수입자가 데이터 주체의 요청을 거부하려는 경우, 데이터 주체에게 거부 이유와 관할 감독 기관에 불만을 제기하거나 사법적 구제를 요청할 수 있는 가능성을 알려야 합니다.

제 11 항

대상

- (a) 데이터 수입자는 개별 통지 또는 웹 사이트를 통해 투명하고 쉽게 액세스할 수 있는 형식으로 불만 사항을 처리할 권한이 있는 연락처를 데이터 주체에게 알려야 합니다. 정보 주체로부터 접수된 모든 불만 사항을 신속하게 처리해야 합니다.
- (b) 본 조항의 준수와 관련하여 데이터 주체와 당사자 중 한 명 간에 분쟁이 발생하는 경우, 해당 당사자는 적시에 문제를 우호적으로 해결하기 위해 최선을 다해야 합니다. 당사자들은 이러한 분쟁에 대해 서로에게 알리고 적절한 경우 분쟁 해결에 협력해야 합니다.
- (c) 데이터 주체가 제 3 항에 따라 제 3 자 수혜자 권리를 행사하는 경우, 데이터 수입자는 다음 사항에 따라 데이터 주체의 결정을 수락해야 합니다.
 - (i) 상시 거주지 또는 근무지의 회원국 감독 당국 또는 제 13 항에 따른 관할 감독 당국에 불만을 제기할 수 있습니다.
 - (ii) 제 18 항의 의미 내에서 분쟁을 관할 법원에 회부합니다.
- (d) 당사자는 데이터 주체가 규정(EU) 2016/679 의 80(1)항에 명시된 조건에 따라 비영리 단체, 조직 또는 협회에 의해 대표될 수 있음을 인정합니다.
- (e) 데이터 수입자는 해당 EU 또는 회원국 법률에 따라 구속력이 있는 결정을 준수해야 합니다.
- (f) 데이터 수입자는 데이터 주체의 선택이 관련 법률에 따라 구제책을 모색할 수 있는 실질적 및 절차적 권리를 침해하지 않는다는 데 동의합니다.

제 12 항

책임

- (a) 각 당사자는 본 조항의 위반으로 인해 상대방 당사자에게 발생한 모든 손해에 대해 상대방 당사자에게 책임을 집니다.
- (b) 각 당사자는 데이터 주체에 대해 책임을 지며, 데이터 주체는 당사자가 본 조항에 따른 제 3 자 수혜자 권리를 침해하여 데이터 주체에게 초래한 물질적 또는 비물질적 손해에 대해 보상을 받을 자격이 있습니다. 이는 규정(EU) 2016/679 에 따른 데이터 수출자의 책임을 침해하지 않습니다.
- (c) 본 조항의 위반으로 인해 데이터 주체에게 발생한 손해에 대해 둘 이상의 당사자가 책임이 있는 경우, 모든 책임 당사자는 공동으로 개별적으로 책임을 져야 하며 데이터 주체는 이러한 당사자를 상대로 법원에 소송을 제기할 수 있습니다.
- (d) 당사자는 한 당사자가 (c)항에 따라 책임을 지는 경우 손해에 대한 책임에 해당하는 보상의 일부를 다른 당사자에게 청구할 수 있음에 동의합니다.
- (e) 데이터 수입자는 자신의 책임을 피하기 위해 처리자 또는 하위 처리자의 행위를 요청할 수 없습니다.

제 13 항

감독

- (a) 부록 I.C.에 명시된 대로 데이터 전송과 관련하여 데이터 수출자가 규정(EU) 2016/679 를 준수하도록 할 책임이 있는 감독 기관이 관할 감독 기관 역할을 합니다.
- (b) 데이터 수입자는 본 조항을 준수하기 위한 모든 절차에서 관할 감독 기관의 관할권에 복종하고 협력하는 데 동의합니다. 특히, 데이터 수입자는 문의에 응답하고, 감사에 제출하고, 시정 및 보상 조치를 포함하여 감독 기관에서 채택한 조치를 준수하는 데 동의합니다. 필요한 조치가 취해졌다는 서면 확인서를 감독 기관에 제공해야 합니다.

섹션 III – 공공 기관이 접근하는 경우의 현지 법률 및 의무

제 14 항

조항 준수에 영향을 미치는 현지 법률 및 관행

- (a) 양 당사자는 개인 데이터 공개 요구 사항 또는 공공 기관의 액세스를 승인하는 조치를 포함하여 데이터 수입자의 개인 데이터 처리에 적용되는 제 3 국의 법률 및 관행이 데이터 수입자가 본 조항에 따른 의무를 이행하는 데 방해가 된다고 믿을 이유가 없음을 보증합니다. 이는 기본권과 자유의 본질을 존중하고 규정(EU) 2016/679 의 23(1)조에 나열된 목표 중 하나를 보호하기 위해 민주주의 사회에서 필요하고 비례하는 수준을 초과하지 않는 법률과 관행이 이 조항과 모순되지 않는다는 이해에 근거합니다.
- (b) 당사자는 (a)항에서 보증을 제공할 때 특히 다음 요소를 충분히 고려했음을 선언합니다.
- (i) 처리 체인의 길이, 관련된 행위자 수 및 사용된 전송 채널을 포함한 전송의 특정 상황; 의도된 제삼자 전송; 수신자 유형; 처리 목적; 전송된 개인 데이터의 범주 및 형식; 이전이 발생하는 경제 부문; 전송된 데이터의 저장 위치;
 - (ii) 공공 기관에 대한 데이터 공개를 요구하거나 해당 당국의 액세스를 승인하도록 요구하는 것을 포함하여 제 3 국의 법률 및 관행은 전송의 특정 상황과 적용 가능한 제한 및 보호 조치에 비추어 관련이 있습니다.
 - (iii) 본 조항에 따른 보호 조치를 보완하기 위해 마련된 모든 관련 계약, 기술 또는 조직적 보호 조치(전송 중 및 목적지 국가에서의 개인 데이터 처리에 적용되는 조치 포함).
- (c) 데이터 수입업자는 (b)항에 따른 평가를 수행할 때 데이터 수출업자에게 관련 정보를 제공하기 위해 최선을 다했음을 보증하며 본 조항을 준수하기 위해 데이터 수출업자와 계속 협력할 것에 동의합니다.
- (d) 당사자들은 (b)항에 따른 평가를 문서화하고 요청 시 관할 감독 기관에 제공하는 데 동의합니다.
- (e) 데이터 수입자는 본 조항에 동의한 후 계약 기간 동안 제 3 국 법률의 변경 또는 해당 법률의 적용을 나타내는 조치(예: 공개 요청)를 포함하여 (a)항의 요구 사항에 부합하지 않는 법률 또는 관행의 적용을 받거나 적용받았다고 믿을 만한 이유가 있는 경우 데이터 수출자에게 즉시 통지하는 데 동의합니다. 단락 (a)의 요구 사항에 부합하지 않는 관행.
- (f) (e)항에 따른 통지 후 또는 데이터 수출업자가 데이터 수입업자가 본 조항에 따른 의무를 더 이상 이행할 수 없다고 믿을 만한 이유가 있는 경우, 데이터 수출업자는 상황을 해결하기 위해 데이터 수출업자 및/또는 데이터 수입업자가 채택할 적절한 조치(예: 보안 및 기밀성 보장을 위한 기술적 또는 조직적 조치)를 즉시 식별해야 합니다. 데이터 수출자는 데이터 전송에 대한 적절한 보호 조치를 보장할 수 없다고 판단하거나 관할 감독 기관의 지시가 있는 경우 데이터

전송을 일시 중단해야 합니다. 이 경우 데이터 수출자는 본 조항에 따른 개인 데이터 처리와 관련된 한 계약을 해지할 수 있습니다. 계약에 두 명 이상의 당사자가 관련된 경우 데이터 수출자는 당사자가 달리 합의하지 않는 한 관련 당사자에 대해서만 이 해지 권리를 행사할 수 있습니다. 본 조항에 따라 계약이 종료되는 경우 16(d)항 및 (e)항이 적용됩니다.

제15 항

공공 기관이 액세스하는 경우 데이터 수입자의 의무

15.1 통지

- (a) 데이터 수입자는 다음과 같은 경우 데이터 수출업자 및 가능한 경우 데이터 주체에게 즉시(필요한 경우 데이터 수출업자의 도움을 받아) 통지하는 데 동의합니다.
 - (i) 본 조항에 따라 전송된 개인 데이터의 공개에 대해 목적지 국가의 법률에 따라 사법 당국을 포함한 공공 기관으로부터 법적 구속력이 있는 요청을 받는 경우 이러한 통지에는 요청된 개인 데이터, 요청 기관, 요청의 법적 근거 및 제공된 응답에 대한 정보가 포함됩니다. 또는
 - (ii) 목적지 국가의 법률에 따라 본 조항에 따라 전송된 개인 데이터에 대한 공공 기관의 직접적인 접근을 인지합니다. 이러한 통지에는 수입업자가 사용할 수 있는 모든 정보가 포함되어야 합니다.
- (b) 데이터 수입업자가 대상 국가의 법률에 따라 데이터 수출업자 및/또는 데이터 주체에게 통지하는 것이 금지된 경우, 데이터 수입업자는 가능한 한 빨리 최대한 많은 정보를 전달하기 위해 금지 면제를 얻기 위해 최선의 노력을 다하는 데 동의합니다. 데이터 수입자는 데이터 수출자의 요청에 따라 이를 입증할 수 있도록 최선의 노력을 문서화하는 데 동의합니다.
- (c) 목적지 국가의 법률에 따라 허용되는 경우, 데이터 수입업자는 계약 기간 동안 정기적으로 데이터 수출업자에게 수신된 요청에 대해 가능한 한 많은 관련 정보(특히 요청 수, 요청된 데이터 유형, 요청 기관, 요청 이의 제기 여부 및 해당 이의 제기 결과, 등).
- (d) 데이터 수입자는 계약 기간 동안 (a)항부터 (c)항까지에 따라 정보를 보존하고 요청 시 관할 감독 기관에 제공하는 데 동의합니다.
- (e) (a)항부터 (c)항은 14(e)항 및 16 항에 따라 데이터 수출업자가 이러한 조항을 준수할 수 없는 경우 데이터 수출업자에게 즉시 알려야 하는 데이터 수입업자의 의무를 침해하지 않습니다.

15.2 합법성 및 데이터 최소화 검토

- (a) 데이터 수입자는 공개 요청의 적법성, 특히 공개 요청이 요청하는 공공 기관에 부여된 권한 내에 있는지 여부를 검토하고, 신중한 평가 후 요청이 목적지 국가의 법률에 따라 불법이라고 간주할 합리적인 근거가 있다고 결론을 내리는 경우 요청에 이의를 제기하는 데 동의합니다. 국제법 및 국제 평등 원칙에 따른 적용 가능한 의무. 데이터 수입자는 동일한 조건 하에서 항소

가능성을 추구해야 합니다. 요청에 이의를 제기하는 경우, 데이터 수입자는 관할 사법 당국이 그 타당성을 결정할 때까지 요청의 효력을 정지하기 위한 임시 조치를 모색해야 합니다. 해당 절차 규칙에 따라 요구될 때까지 요청된 개인 데이터를 공개하지 않습니다. 이러한 요구 사항은 14(e)항에 따른 데이터 수입자의 의무를 침해하지 않습니다.

- (b) 데이터 수입자는 법적 평가 및 공개 요청에 대한 이의 제기를 문서화하고, 대상 국가의 법률이 허용하는 범위 내에서 데이터 수출자가 문서를 사용할 수 있도록 하는 데 동의합니다. 또한 요청 시 관할 감독 기관에서 사용할 수 있도록 해야 합니다.
- (c) 데이터 수입자는 공개 요청에 응답할 때 요청에 대한 합리적인 해석에 따라 허용되는 최소한의 정보를 제공하는 데 동의합니다.

섹션 IV – 최종 조항

제 16 항

조항 미준수 및 해지

- (a) 데이터 수입업자는 어떤 이유로든 본 조항을 준수할 수 없는 경우 데이터 수출업자에게 즉시 알려야 합니다.
- (b) 데이터 수입업자가 본 조항을 위반하거나 준수할 수 없는 경우 데이터 수출업자는 규정 준수가 다시 보장되거나 계약이 종료될 때까지 데이터 수입업자에 대한 개인 데이터 전송을 일시 중단해야 합니다. 이는 14(f)항을 침해하지 않습니다.
- (c) 데이터 수출자는 다음과 같은 경우 본 조항에 따른 개인 데이터 처리와 관련하여 계약을 해지할 수 있습니다.
 - (i) 데이터 수출자가 (b)항에 따라 데이터 수입자에 대한 개인 데이터 전송을 일시 중단했으며 본 조항의 준수가 합리적인 시간 내에 어떠한 경우에도 일시 중지 후 1 개월 이내에 복원되지 않은 경우
 - (ii) 데이터 수입업자가 본 조항을 실질적으로 또는 지속적으로 위반하는 경우 또는
 - (iii) 데이터 수입자가 본 조항에 따른 의무에 대한 관할 법원 또는 감독 기관의 구속력 있는 결정을 준수하지 않는 경우.

이러한 경우 관할 감독 기관에 그러한 불이행을 통보해야 합니다. 계약에 두 명 이상의 당사자가 관련된 경우 데이터 수출자는 당사자가 달리 합의하지 않는 한 관련 당사자에 대해서만 이 해지 권리를 행사할 수 있습니다.

- (d) (c)항에 따라 계약이 종료되기 전에 전송된 개인 데이터는 데이터 수출업자의 선택에 따라 즉시 데이터 수출자에게 반환되거나 완전히 삭제되어야 합니다. 모든 데이터 사본에도 동일하게 적용됩니다. 데이터 수입업자는 데이터 수출업자에게 데이터 삭제를 인증해야 합니다. 데이터가 삭제되거나 반환될 때까지 데이터 수입자는 본 조항을 계속 준수해야 합니다. 전송된 개인 데이터의 반환 또는 삭제를 금지하는 데이터 수입자에게 적용되는 현지 법률의 경우, 데이터 수입자는 본 조항을 계속 준수하고 해당 현지 법률에서 요구하는 범위 및 기간 동안만 데이터를 처리할 것임을 보증합니다.
- (e) 각 당사자는 (i) 유럽연합 집행위원회가 규정(EU) 2016/679 의 45(3)조에 따라 본 조항이 적용되는 개인 데이터의 전송에 관한 결정을 채택하는 경우 본 조항에 구속되는 계약을 철회할 수 있습니다. 또는 (ii) 규정 (EU) 2016/679 는 개인 데이터가 전송되는 국가의 법적 프레임워크의 일부가 됩니다. 이는 규정(EU) 2016/679 에 따라 해당 처리에 적용되는 다른 의무를 침해하지 않습니다.

제 17 항

준거법

본 조항은 EU 회원국 중 한 곳의 법률이 적용되며, 해당 법률은 제 3 자 수혜자 권리를 허용합니다. 당사자들은 이것이 독일의 법률이라는 데 동의합니다.

제 18 항

관할권 및 관할권 선택

- (a) 본 조항으로 인해 발생하는 모든 분쟁은 EU 회원국의 법원에서 해결해야 합니다.
- (b) 당사자들은 이러한 법원이 독일의 법원이라는 데 동의합니다.
- (c) 또한 데이터 주체는 데이터 수출업자 및/또는 데이터 수입업자를 상대로 상시 거주지가 있는 회원국의 법원에 법적 소송을 제기할 수 있습니다.
- (d) 당사자들은 그러한 법원의 관할권에 복종하는 데 동의합니다.

부록

설명 참고 사항:

각 전송 또는 전송 범주에 적용되는 정보를 명확하게 구별할 수 있어야 하며, 이와 관련하여 데이터 수출자 및/또는 데이터 수입자로서 당사자의 각 역할을 결정할 수 있어야 합니다. 이를 위해 각 양도/양도 범주 및/또는 계약 관계에 대해 별도의 부록을 작성하고 서명할 필요는 없으며, 이러한 투명성은 하나의 부록을 통해 달성될 수 있습니다. 그러나 충분한 명확성을 보장하기 위해 필요한 경우 별도의 부록을 사용해야 합니다.

부록 I

A.당사자 목록

데이터 수출자:

1. 이름: 메르세데스-벤츠 AG

주소: 메르세데스슈트라 세(Mercedesstraße) 120

담당자의 이름, 직위 및 연락처 정보: /

본 조항에 따라 전송된 데이터와 관련된 활동: 아래 B.를 참조하십시오.

서명 및 날짜: 이 파트 A 의 섹션 5 를 참조하십시오.

역할(컨트롤러/프로세서): 컨트롤러

데이터 수입자:

1. 이름: ASP(계약의 루브럼 참조)

주소: 협정의 루브럼 참조

담당자의 이름, 직위 및 연락처 정보: /

본 조항에 따라 전송된 데이터와 관련된 활동: 아래 B.를 참조하십시오.

서명 및 날짜: 가입 절차 세부 정보 및 문서를 참조하십시오.

역할(컨트롤러/프로세서): 컨트롤러

B.전송에 대한 설명

개인 데이터가 전송되는 데이터 주체의 범주

파트 A 의 부록 1 참조

전송되는 개인 데이터의 범주

파트 A 의 부록 1 참조

민감한 데이터 전송(해당되는 경우) 및 데이터의 특성 및 관련 위험을 완전히 고려한 제한 또는 보호 조치를 적용한 경우(예: 엄격한 목적 제한, 액세스 제한(전문 교육을 이수한 직원에 대한 액세스 포함), 데이터에 대한 액세스 기록 유지, 제삼자 전송 제한 또는 추가 보안 조치).

해당 사항 없음

전송 빈도(예: 데이터가 일회성 또는 연속적으로 전송되는지 여부).

연속 기준

처리의 성격

파트 A 의 부록 1 참조

데이터 전송 및 추가 처리의 목적

파트 A 의 부록 1 참조

개인 데이터가 보존되는 기간 또는 가능하지 않은 경우 해당 기간을 결정하는 데 사용되는 기준

| | | |
|--|-----------------------|--|
| 고객 데이터: 회사 직위, 사용자 이름, 사용자 ID, 주소, 이메일, 전화, 주문 세부 정보(주문일, 주문한 부품/서비스, 주문 수량, 판매, 주문 미주문(판매 손실), B2B Connect 플랫폼 사용 빈도, 배송 시간 등 ISP/ISP 직원) | 비즈니스 프로세스에서 리텐션 기간 정의 | 주문 후 2 년 후 익명화, 보고서 작성 후 3 년 후 삭제(월별 및 분기별 보고서 작성) |
| | 특정 시작 날짜가 있는 삭제 규칙 | 주문 후 2 년 후 익명화, 월간 또는 분기별 보고서 생성 후 3 년 후 삭제 |

(하위) 처리자로의 전송의 경우, 처리의 주제, 성격 및 기간도 명시합니다

해당 사항 없음

C.관할 감독 기관

제 13 항에 따라 관할 감독 기관을 식별합니다.

*Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Königstraße 10 a, 70173
슈투트가르트*

부록 II - 데이터 보안을 보장하기 위한 기술적 및 조직적 조치를 포함한 기술적 및 조직적 조치

설명 참고 사항:

기술적 및 조직적 조치는 구체적인(일반적이 아닌) 용어로 설명되어야 합니다. 또한 부록의 첫 페이지에 있는 일반적인 의견, 특히 각 전송/전송 집합에 적용되는 조치를 명확하게 표시해야 할 필요성에 대한 설명을 참조하십시오.

데이터 수입자가 적절한 수준의 보안을 보장하기 위해 구현한 기술적 및 조직적 조치(관련 인증 포함)에 대한 설명, 처리의 성격, 범위, 컨텍스트 및 목적, 자연인의 권리와 자유에 대한 위험을 고려합니다.

B2B Connect 관련 처리 활동(비즈니스 분석 및 캠페인/마케팅 지원 포함)의 경우 다음 TOM 이 적용됩니다.

| 1. 출입 통제(물리적) | 예 | 아니요 | 해당 사항 없음 |
|--|-------------------------------------|--------------------------|--------------------------|
| 애플리케이션이 개인 데이터를 처리하는 시스템이 있는 영역은 여러 보안 영역으로 나뉩니다 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 관련 방 또는 구역에 대한 물리적 접근에 관한 권한 범위를 포함한 승인된 사람의 지정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 발급된 입장 허가 ID | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 방문자를 위한 규칙 및 규정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 구현된 키를 관리하는 규칙 및 규정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 안팎으로 기록된 모든 개인 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 회사 구내의 물리적 보호(예: 울타리, 외벽, 검문소) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 안전한 입구(예: 잠금 시스템, ID 리더기) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 도난 방지 창문 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 감시 설치(예: 경보 시스템, CCTV) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 분리 시스템(예: 개찰구, 양문 시스템) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 물리적 보호 조치에 대한 문서화 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| 2. 출입 통제(시스템) | 예 | 아니요 | 해당 사항 없음 |
|---|-------------------------------------|--------------------------|-------------------------------------|
| 응용 프로그램 입력(로그인)을 위한 문서화된 보안 개념 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| GAS(Global Authentication Service) 사용 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 회사 디렉터리와 정기적인 동기화 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| SAGW/WCP(Secure Application Gateway) 사용 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 접근 권한 지정 및 확인 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 사용자 식별 및 권한 확인 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 사용자 ID 관리 시스템 구현 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 특수 인증 프로세스(예: 칩 카드, 생체 인식 액세스 제어) | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 적절한 암호 보호(보안 암호, 암호화된 저장소에 대한 구속력 있는 요구 사항) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 보안 문제에 대한 대응을 포함하여 모니터링되는 액세스 시도 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| | | | |
|-------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| 내부 네트워크 격리(예: VPN, 방화벽 사용) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 전직 직원의 계정 즉시 삭제 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 특수 보안 소프트웨어(예: 맬웨어 방지, 침입 탐지) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 방문자를 위한 규칙 및 규정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 원격 접근 규칙 및 규정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| 3. 액세스 제어(사용자 권한) | 예 | 아니요 | 해당 사항 없음 |
|--|-------------------------------------|-------------------------------------|--------------------------|
| 응용 프로그램에 대해 구현된 권한 부여 및 역할 개념 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 액세스에 필요한 사용자 계정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 승인에 대한 정기 검토 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 부과된 접근 제한(알아야 할 사항 및 최소 권한의 원칙에 기반) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 특히 중요한 기능(예: 시스템 관리자)을 위한 추가 암호(4-eyes-principle 기반) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 시스템의 다중 클라이언트 기능 확보 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 분리된 다중 클라이언트 지원 데이터베이스 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 개발, 테스트, 통합 및 생산 환경의 분리 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 생산 환경과 아카이빙 환경의 분리 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 읽기 액세스 기록됨 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 쓰기 액세스 기록 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 기록된 무단 액세스 시도 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 보존 기간 구현 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| 4. 공시 통제 | 예 | 아니요 | 해당 사항 없음 |
|--|-------------------------------------|-------------------------------------|-------------------------------------|
| 암호화된 데이터 전송 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 보존 암호화 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 모바일 단말기 암호화(예: 하드 디스크 암호화) | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 데이터 전달 또는 전송이 기록됨 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 완전히 문서화된 데이터 전달 형식(예: 인쇄물, 데이터 미디어, 자동 전송) | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 문서화된 인터페이스 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 전송에 대한 권한 제한 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 수행된 데이터에 대한 타당성, 완전성 및 정확성 검사 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| USB 인터페이스 비활성화 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 모바일 기기 취급 규정 시행 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 데이터 캐리어 폐기 규정 시행 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 조작으로부터 보호(맬웨어 방지) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| 5. 입력 제어 | 예 | 아니요 | 해당 사항 없음 |
|---|-------------------------------------|-------------------------------------|-------------------------------------|
| 시스템 로깅/기록 보장 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 로그 파일/프로토콜의 정기 평가 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| SoD(Segregation of Duties) 보장 (SoD 매트릭스 정의 및 절차 구현) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 문서화된 데이터를 입력, 변경 또는 삭제할 수 있는 권한 부여 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 완전히 기록/기록된 데이터의 입력/변경 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 부분적으로 기록/기록된 데이터의 입력/변경 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 변경/삭제 금지 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 변경의 신뢰성을 보장하기 위한 전자 서명 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

| 6. 작업 제어 | 예 | 아니요 | 해당 사항 없음 |
|--|-------------------------------------|-------------------------------------|--------------------------|
| Mercedes-Benz 의 데이터 처리에 대한 표준 계약이 합의되었습니다. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 대리인의 데이터 처리에 대한 데이터 처리자의 표준 계약이 합의되었습니다. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| EU 집행위원회의 표준 계약 조항은 제 3 국의 처리자가 대신 데이터를 처리하도록 합의되었습니다. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 컨트롤러와 데이터 프로세서의 책임은 엄격하게 규제/분리됩니다. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 프로세서에 제공된 지침을 조정/변경하기 위해 지정된 규칙 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 현장 통제는 데이터 컨트롤러에 의해 수행되고 문서화되었습니다 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 데이터 프로세서가 제출한 자체 평가 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 데이터 처리자가 제출한 승인된 인증 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 데이터 처리자가 제출한 하도급업체 목록 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 처리업체별 하도급업체 확인 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

| 7. 가용성 제어 | 예 | 아니요 | 해당 사항 없음 |
|---------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| 시스템 상태를 정기적으로 확인(모니터링) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 백업 및 복구 계획 수립(정기적인 데이터 백업) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 구현된 데이터 아카이빙 전략 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 문서화된 비상 계획(비즈니스 연속성, 재해 복구) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 정기적으로 테스트되는 비상 계획 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 평가된 중복 IT 시스템의 존재 여부(서버, 스토리지 등) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 완벽하게 작동하는 물리적 보호 시스템(화재 방지, 에너지, A/C) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| 8. 취해진 기술적 및 조직적 조치의 효과에 대한 정기적인 검토, 평가 및 평가 절차 | 예 | 아니요 | 해당 사항 없음 |
|---|-------------------------------------|--------------------------|--------------------------|
| 시스템 상태 정기 점검(모니터링) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 설명된 조치의 이행 개정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| | | | |
|--|-------------------------------------|--------------------------|--------------------------|
| 구속력 있는 지침 및 조치 지침에서 적용 가능한 데이터 보호 요구 사항에 대한 설명 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 관련 새로운 데이터 처리 절차에 대한 데이터 보호 책임자의 참여 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Webparts 관련 처리 활동(비즈니스 분석 및 캠페인/마케팅 지원 포함)의 경우 다음 TOM 이 적용됩니다.

| 1. 출입 통제(물리적) | 예 | 아니요 | 해당 사항 없음 |
|--|-------------------------------------|--------------------------|-------------------------------------|
| 애플리케이션이 개인 데이터를 처리하는 시스템이 있는 영역은 여러 보안 영역으로 나뉩니다 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 관련 방 또는 구역에 대한 물리적 접근에 관한 권한 범위를 포함한 승인된 사람의 지정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 발급된 입장 허가 ID | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 방문자를 위한 규칙 및 규정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 구현된 키를 관리하는 규칙 및 규정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 안팎으로 기록된 모든 개인 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 회사 구내의 물리적 보호(예: 울타리, 외벽, 검문소) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 안전한 입구(예: 잠금 시스템, ID 리더기) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 도난 방지 창문 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 감시 설치(예: 경보 시스템, CCTV) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 분리 시스템(예: 개찰구, 양문 시스템) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 물리적 보호 조치에 대한 문서화 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| 2. 출입 통제(시스템) | 예 | 아니요 | 해당 사항 없음 |
|---|-------------------------------------|-------------------------------------|--------------------------|
| 응용 프로그램 입력(로그인)을 위한 문서화된 보안 개념 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| GAS(Global Authentication Service) 사용 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 회사 디렉터리와 정기적인 동기화 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| SAGW/WCP(Secure Application Gateway) 사용 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 접근 권한 지정 및 확인 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 사용자 식별 및 권한 확인 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 사용자 ID 관리 시스템 구현 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 특수 인증 프로세스(예: 칩 카드, 생체 인식 액세스 제어) | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 적절한 암호 보호(보안 암호, 암호화된 저장소에 대한 구속력 있는 요구 사항) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 보안 문제에 대한 대응을 포함하여 모니터링되는 액세스 시도 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 내부 네트워크 격리(예: VPN, 방화벽 사용) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 전직 직원의 계정 즉시 삭제 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 특수 보안 소프트웨어(예: 맬웨어 방지, 침입 탐지) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 방문자를 위한 규칙 및 규정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 원격 접근 규칙 및 규정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| 3. 액세스 제어(사용자 권한) | 예 | 아니요 | 해당 사항 없음 |
|-------------------------------|-------------------------------------|--------------------------|--------------------------|
| 응용 프로그램에 대해 구현된 권한 부여 및 역할 개념 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| | | | |
|--|-------------------------------------|-------------------------------------|-------------------------------------|
| 데이터 액세스에 필요한 사용자 계정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 승인에 대한 정기 검토 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 부과된 접근 제한(알아야 할 사항 및 최소 권한의 원칙에 기반) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 특히 중요한 기능(예: 시스템 관리자)을 위한 추가 암호(4-eyes-principle 기반) | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 시스템의 다중 클라이언트 기능 확보 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 분리된 다중 클라이언트 지원 데이터베이스 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 개발, 테스트, 통합 및 생산 환경의 분리 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 생산 환경과 아카이빙 환경의 분리 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 읽기 액세스 기록됨 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 쓰기 액세스 기록 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 기록된 무단 액세스 시도 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 데이터 보존 기간 구현 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

| 4. 공시 통제 | 예 | 아니요 | 해당 사항 없음 |
|--|-------------------------------------|--------------------------|-------------------------------------|
| 암호화된 데이터 전송 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 보존 암호화 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 모바일 단말기 암호화(예: 하드 디스크 암호화) | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 데이터 전달 또는 전송이 기록됨 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 완전히 문서화된 데이터 전달 형식(예: 인쇄물, 데이터 미디어, 자동 전송) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 문서화된 인터페이스 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 전송에 대한 권한 제한 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 수행된 데이터에 대한 타당성, 완전성 및 정확성 검사 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| USB 인터페이스 비활성화 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 모바일 기기 취급 규정 시행 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 데이터 캐리어 폐기 규정 시행 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 데이터 조작으로부터 보호(맬웨어 방지) | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

| 5. 입력 제어 | 예 | 아니요 | 해당 사항 없음 |
|--|-------------------------------------|-------------------------------------|-------------------------------------|
| 시스템 로깅/기록 보장 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 로그 파일/프로토콜의 정기 평가 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| SoD(Segregation of Duties) 보장(SoD 매트릭스 정의 및 절차 구현) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 문서화된 데이터를 입력, 변경 또는 삭제할 수 있는 권한 부여 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 완전히 기록/기록된 데이터의 입력/변경 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 부분적으로 기록/기록된 데이터의 입력/변경 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 변경/삭제 금지 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

| | | | |
|----------------------------|--------------------------|-------------------------------------|--------------------------|
| 데이터 변경의 신뢰성을 보장하기 위한 전자 서명 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
|----------------------------|--------------------------|-------------------------------------|--------------------------|

| 6. 작업 제어 | 예 | 아니요 | 해당 사항 없음 |
|--|-------------------------------------|-------------------------------------|-------------------------------------|
| Mercedes-Benz 의 데이터 처리에 대한 표준 계약이 합의되었습니다. | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 대리인의 데이터 처리에 대한 데이터 처리자의 표준 계약이 합의되었습니다. | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| EU 집행위원회의 표준 계약 조항은 제 3 국의 처리자가 대신 데이터를 처리하도록 합의되었습니다. | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 데이터 컨트롤러와 데이터 프로세서의 책임은 엄격하게 규제/분리됩니다. | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 데이터 프로세서에 제공된 지침을 조정/변경하기 위해 지정된 규칙 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 현장 통제는 데이터 컨트롤러에 의해 수행되고 문서화되었습니다 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 데이터 프로세서가 제출한 자체 평가 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 데이터 처리자가 제출한 승인된 인증 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 데이터 처리자가 제출한 하도급업체 목록 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 처리업체별 하도급업체 확인 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

| 7. 가용성 제어 | 예 | 아니요 | 해당 사항 없음 |
|---------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| 시스템 상태를 정기적으로 확인(모니터링) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 백업 및 복구 계획 수립(정기적인 데이터 백업) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 구현된 데이터 아카이빙 전략 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 문서화된 비상 계획(비즈니스 연속성, 재해 복구) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 정기적으로 테스트되는 비상 계획 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 평가된 중복 IT 시스템의 존재 여부(서버, 스토리지 등) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 완벽하게 작동하는 물리적 보호 시스템(화재 방지, 에너지, A/C) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| 8. 취해진 기술적 및 조직적 조치의 효과에 대한 정기적인 검토, 평가 및 평가 절차 | 예 | 아니요 | 해당 사항 없음 |
|---|-------------------------------------|--------------------------|--------------------------|
| 시스템 상태 정기 점검(모니터링) | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 설명된 조치의 이행 개정 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 구속력 있는 지침 및 조치 지침에서 적용 가능한 데이터 보호 요구 사항에 대한 설명 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 관련 새로운 데이터 처리 절차에 대한 데이터 보호 책임자의 참여 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

파트 B

컨트롤러를 대신하는 데이터 처리에 관한 조항

서문

컨트롤러를 대신하는 데이터 처리에 관한 본 조항("조항 파트 B")은 아래에 설명된 대로 컨트롤러를 대신하여 데이터 처리로 인해 발생하는 데이터 보호와 관련된 당사자의 의무를 명시합니다. 파트 B의 이러한 조항은 이러한 처리 작업과 관련된 모든 활동에 적용되며 그 과정에서 처리자 또는 처리자가 위탁한 제 3자가 관리자의 개인 데이터와 접촉할 수 있습니다. 그러나 이 조항은 당사자 중 한 명이 다른 당사자에 대해 GDPR 28 항의 의미에서 처리자 역할을 하는 상황으로 적용이 제한됩니다. 이 범위를 벗어나면 이 조항은 적용되지 않습니다.

1. 역할 및 책임

관리자는 A/S 사업을 수행하기 위해 개인 데이터 처리에 의존합니다. 이를 위해 프로세서는 부록 1에 설명된 대로 컨트롤러에 서비스를 제공합니다.

2. 주제 및 책임

프로세서는 컨트롤러를 대신하여 개인 데이터를 처리합니다. 커미셔닝의 주제는 아래에 명시된 활동 또는 추가 서비스 계약 또는 주문 양식에 명시된 활동입니다. 본 조항 파트 B의 범위 내에서 관리자는 관련 데이터 보호법 준수, 특히 처리자로의 데이터 전송의 적법성, 처리자를 통한 데이터 처리 및 서비스 과정에서 후속 데이터 처리에 대해 전적으로 책임을 집니다.

3. 위임의 명세

- 3.1 개인 데이터의 위탁된 수집, 처리 및/또는 사용의 목적, 유형 및 범위는 부록 1에 자세히 설명되어 있습니다.
- 3.2 수집 및/또는 사용되는 개인 데이터의 유형 및 범주와 본 계약에 따라 개인 데이터를 취급하는 데이터 주체의 범주는 부록 1에 자세히 설명되어 있습니다.

4. 지시를 내릴 수 있는 관리자의 권리

- 4.1 커미셔닝 범위 내에서 관리자는 개별 지침을 발행하여 지정할 수 있는 데이터 처리의 유형, 범위 및 절차에 관한 지침을 발행할 권리가 있습니다. 이는 결정적으로 결정되며 제공된 응용 프로그램 및 시스템에서 제공하는 설정 및 기능을 통해 실행되어야 합니다. 합의된 처리 주제 및 절차의 변경으로 이어지는 지침은 합의되어야 하며 문서화되어야 합니다.
- 4.2 프로세서는 데이터 보호 요구 사항을 위반하는 것으로 간주되는 모든 지침을 컨트롤러에 알립니다. 그런 다음 프로세서는 컨트롤러가 서면(이메일 포함)으로 확인하거나 변경할 때까지 관련 명령의 실행을 연기할 수 있습니다.
- 4.3 당사자 간에 서면으로 작성된 편차 계약을 제외하고, 관리자의 경영진 또는 기타 권한을 위임받은 대리인만이 관리자 측에서 서면(이메일 포함)으로 지침을 발행할 권한이 있습니다.

4.4 처리자 측의 지시를 받을 수 있는 권한이 있는 사람은 mbk_dataprotection@mercedes-benz.com 를 통해 연락할 수 있는 "MBK 의 데이터 보호 책임자를 위한 데이터 보호 코디네이터"입니다.

5. 처리자의 의무

5.1 프로세서는 유럽 연합 또는 회원국 법률 또는 프로세서가 적용되는 기타 관련 데이터 보호법에 의해 요구되지 않는 한 컨트롤러가 위임하고 컨트롤러의 지시에 따라 데이터를 수집하거나 처리해야 합니다. 이러한 경우, 처리자는 해당 법률이 중요한 공익적 근거로 해당 정보를 금지하지 않는 한 처리 전에 해당 법적 요구 사항을 컨트롤러에게 알려야 합니다.

프로세서는 컨트롤러의 지시에 따라서만 컨트롤러를 대신하여 처리된 데이터를 수정, 삭제 또는 차단합니다. 데이터 주체가 데이터 수정 또는 삭제를 요청하기 위해 프로세서에 연락하는 경우, 프로세서는 요청을 컨트롤러에게 전달해야 합니다.

5.2 관련 법률이나 법 집행 기관의 법적 구속력이 있는 요청에 의해 금지되지 않는 한, 프로세서는 데이터 보호 감독 기관, 법 집행 기관 또는 기타 공공 기관의 개인 데이터에 대한 액세스 또는 압수 요청을 컨트롤러에게 즉시 알려야 합니다. 또한 법이 허용하는 한도 내에서 프로세서는 그러한 조치를 방어하거나 컨트롤러가 프로세서를 대신하여 방어할 수 있도록 합리적으로 사용 가능한 모든 조치를 취해야 하며, 그렇게 선택하는 경우 보호 명령을 요청하거나 컨트롤러가 프로세서를 대신하여 그렇게 할 수 있도록 허용해야 합니다. 어떠한 경우에도 프로세서는 이러한 방어를 위해 컨트롤러와 합리적으로 협력해야 합니다.

5.3 개인 데이터에 대한 액세스 권한을 부여하기 전에 처리자는 개인 데이터 처리에 고용된 사람에게 데이터 기밀 유지 및 기밀 유지를 의무화하고 본 조항 파트 B 에 명시된 조항 및 이들에게 적용되는 데이터 보호 의무를 숙지해야 합니다. 프로세서가 전문적 기밀 유지 또는 기타 특별 기밀 유지 의무(예: 통신 기밀 유지 대상 데이터)에 따라 개인 데이터를 처리하는 경우, 이러한 의무에는 이러한 특정 상황 및 관련 의무도 포함됩니다.

5.4 관련 데이터 보호법에서 요구하는 한, 프로세서는 데이터 보호 책임자를 임명하고 연락처 세부 정보를 컨트롤러에게 전달하며 본 계약 기간 동안 변경 및 업데이트를 부당한 지체 없이 컨트롤러에 보고해야 합니다.

5.5 처리자는 처리자 또는 처리자가 고용한 사람이 관리자의 개인 데이터를 보호하기 위한 지침 또는 조항을 위반한 경우 부당한 지체 없이 관리자에게 통지합니다.

프로세서는 컨트롤러가 개인 데이터 보호 위반을 문서화하고 필요한 경우 그러한 위반에 대해 72 시간 이내에 데이터 주체 각각에 감독 기관에 알려야 할 의무가 있음을 인정합니다. 그러한 위반이 발생한 경우, 프로세서는 컨트롤러가 본 계약에 따른 의무를 적시에 수행할 수 있도록 적절한 방식으로 보고 의무를 준수하도록 컨트롤러를 지원합니다. 처리자는 관리자에게 위반 사실을 알리고 처리자가 사용할 수 있는 경우 최소한 다음 정보를 제공합니다. (a) 위반의 종류, 범주 및 관련된 데이터 주체 및 데이터 세트의 대략적인 양에 대한 설명, (b) 추가 정보를 위한 담당자의 이름 및 연락처, (c) 위반의 가능한 결과에 대한 설명, (d) 위반을 시정하거나 줄이기 위해 취한 조치에 대한 설명.

또한 프로세서는 정상적인 운영 과정의 심각한 중단, 데이터 보호 위반 또는 컨트롤러의 데이터 처리 중 기타 불규칙성이 의심되는 경우 부당한 지체 없이 컨트롤러에게 알려야 합니다.

5.6 프로세서는 컨트롤러의 개인 데이터 처리와 관련하여 감독 기관이 취한 모든 모니터링 활동 및 조치를 컨트롤러에게 알립니다.

- 5.7 프로세서는 데이터 주체에 대한 컨트롤러의 의무(예: 데이터 주체에 대한 정보 및 액세스, 데이터 수정 및 삭제, 처리 제한 또는 데이터 이동성에 대한 권리 및 반대할 권리)를 이행하기 위해 가능하고 합리적인 범위 내에서 적절한 기술적 및 조직적 조치로 컨트롤러를 지원합니다. 해당되는 경우.
- 5.8 처리자는 데이터 보호 영향 평가 준비를 지원하며, 적절한 경우 감독 기관의 사전 협의를 지원합니다. 컨트롤러의 요청에 따라 프로세서는 필요한 정보와 문서를 컨트롤러에게 공개해야 합니다.
- 5.9 당사자는 위의 5.7 및 5.8 에 따라 발생하는 추가 비용에 대해 합의해야 합니다. MBK 가 제공하는 이러한 서비스에 대한 비용을 부담할 의무는 없으며, MBK 는 성문법에 따라 이러한 위탁의 존재 여부와 관계없이 MBK 가 수행해야 하거나 수행해야 할 의무가 있습니다.
- 5.10 처리자는 위탁된 데이터 처리를 실행하는 동안 위에 명시된 의무 준수 여부를 모니터링해야 합니다.
- 5.11 처리자는 컨트롤러를 대신하여 수행된 처리 활동에 대한 기록을 유지해야 합니다.

6. 처리 보안

- 6.1 처리자는 위험에 적합한 보안 수준을 보장하고 컨트롤러가 관련 데이터 보호법을 준수하도록 지원하기 위해 모든 적절한 기술적 및 조직적 조치를 취합니다.

따라서 책임 범위 내에서 처리자는 모든 해당 데이터 보호 및 데이터 보안 요구 사항에 따라 내부 조직을 구성합니다. 프로세서는 관련 법률에 따른 요구 사항에 따라 오용 및 손실로부터 컨트롤러 데이터를 합리적으로 보호하기 위해 기술적, 조직적 조치를 취, 유지 및 제어해야 합니다.
- 6.2 이와 관련하여 프로세서는 최첨단 기술, 구현 비용, 처리의 성격, 범위, 컨텍스트 및 목적뿐만 아니라 자연인의 권리와 자유에 대한 다양한 가능성과 심각성의 위험을 고려하여 위험에 적합한 수준의 보안을 제공해야 합니다. 여기에는 출입 통제, 사용자 통제, 액세스 제어, 전송 제어, 입력 제어, 작업 제어, 가용성 제어 및 목적별 분리, 특히 개인 데이터의 가명화 및 암호화, 처리 시스템 및 서비스의 지속적인 기밀성, 무결성, 가용성 및 복원력을 보장하는 능력, 적시에 개인 데이터에 대한 가용성 및 액세스를 복원할 수 있는 능력과 같은 적절한 조치가 포함됩니다. 물리적 또는 기술적 사고가 발생한 경우 및 처리의 보안을 보장하기 위한 기술적 및 조직적 조치의 효과를 정기적으로 테스트, 평가 및 평가하는 프로세스.
- 6.3 기술적 및 조직적 조치에 대한 추가 사양은 부록 2 의 결과입니다.
- 6.4 기술적 및 조직적 조치는 기술적 진보 및 발전에 따라 달라질 수 있습니다. 프로세서는 적절한 대체 조치를 시행할 수 있습니다. 그러나 이는 지정된 조치에서 제공하는 보안 수준에 미치지 못해서는 안 됩니다. 그러나 중요한 변경 사항은 문서화해야 합니다.

7. 관리자의 권리와 의무

- 7.1 컨트롤러와 프로세서는 본 계약에 따라 처리될 개인 데이터와 관련하여 둘 중 하나에 적용되는 해당 법적 데이터 보호법을 준수할 책임이 있습니다.
- 7.2 데이터 주체는 컨트롤러(및 프로세서)가 보유한 개인 데이터와 관련하여 다양한 권리를 갖습니다. 어떤 경우에도 데이터 주체와 직접적인 관계가 있는 컨트롤러이기도 하므로, 컨트롤러는 관련 데이터 주체 권리의 적절한 이행을 보장해야 하며, 특히 관련 데이터 보호법에 따라 당사자가 수행하는 역할 및 작업에 대해 데이터 주체에게

적절하게 알리기 위해(예: 고객을 위한 관련 개인 정보 보호 정책의 실제 버전에 대한 액세스 제공) 보장해야 합니다.

7.3 컨트롤러는 제공된 데이터 미디어를 반환하거나 시운전 종료 후 기록된 데이터를 삭제하기 위한 조치를 지정해야 합니다. 사양이 발행되지 않으면 데이터를 컨트롤러에게 전달하거나 파기해야 합니다. 데이터가 특정 사양에 따라 삭제되는 한, 프로세서는 컨트롤러의 요청에 따라 그러한 삭제가 적용된 날짜를 명시하여 컨트롤러에게 그러한 삭제를 확인해야 합니다.

8. 감사

8.1 관리자 또는 그가 임명한 대리인은 정기 검사를 포함하여 본 계약 및 관련 데이터 보호법에 명시된 모든 지침 및 요구 사항의 준수를 통제할 권리가 있습니다. 프로세서는 이러한 제어를 허용하고 컨트롤러를 지원하며 필요한 정보를 제공할 것을 약속합니다.

8.2 관리자는 주로 처리자의 데이터 보호 조직의 데이터 보호 책임자에 의한 각각의 자체 감사 및/또는 독립 감사자의 인증을 요구함으로써 통제 의무를 추구해야 합니다. 관리자는 관련 데이터 보호법에 따라 필요한 경우 추가 현장 검사를 수행할 권리가 있습니다.

8.3 위의 8.1 항 및 8.2 항에 따른 관리자의 감사는 정규 업무 시간 중에 이루어져야 하며, 표준 내부 운영을 방해하지 않아야 하며, 사전에 합리적으로 통지되어야 합니다.

8.4 관리자의 서면 요청에 따라 처리자는 합리적인 기간 내에 관리자에게 정보를 제공하고 감사에 필요한 문서를 제공해야 합니다.

9. 하위 처리자

9.1 처리자는 계약상의 의무를 이행하기 위해 하위 처리자를 사용할 수 있습니다.

9.2 처리자는 하위 처리자와 계약에 따라 계약을 체결하여 하위 처리자가 수행 중에 관리자의 개인 데이터에 대한 액세스 권한을 부여받기 전에 파트 B 의 본 조항에 따라 처리자가 맡은 것과 최소한 실질적으로 동일한 의무를 하위 처리자에게 부과해야 합니다.

9.3 처리자가 하위 처리자를 포함하는 경우, 부록 1 에는 절차별로 관련된 하위 처리자에 대한 추가 정보가 포함되어 있습니다. 또한 관련 하위 처리자는 부록 3 에 나열되어 있습니다. 프로세서는 다른 하위 프로세서의 추가 또는 교체와 관련하여 의도된 변경 사항을 컨트롤러에게 알려야 하며, 이를 통해 컨트롤러는 그러한 변경에 이의를 제기할 수 있는 기회를 제공해야 하며, 컨트롤러는 그러한 이의에 대한 합리적인 근거를 제시해야 합니다. 컨트롤러가 여전히 새로운 하위 프로세서를 승인하지 않는 경우, 컨트롤러와 프로세서는 해지에 대한 서면 통지를 제공하여 위약금 없이 서비스의 영향을 받는 부분을 종료할 수 있습니다.

9.4 본 9 항은 처리자가 보조 서비스를 제 3 자에게 하도급하는 경우에는 적용되지 않습니다. 이러한 보조 서비스에는 우편, 통신, 배송 및 수령 서비스, 간병 서비스가 포함되지만 이에 국한되지 않습니다.

10. 지역 및 국제 데이터 전송

10.1 국제 데이터 전송(있는 경우, 하위 처리자와 관련된 데이터 전송 포함)이 Mercedes-Benz 데이터 보호 지침 EU A 17.4 의 적용을 받지 않는 경우, 당사자들(하위 처리자와 관련해서도 포함)은 필요한 경우 해당 EU 표준 계약 조항을 체결해야 합니다.

10.2 해당되는 경우, EU 표준 계약 조항(부속서 포함)의 조항은 본 조항 파트 B 및 전체 계약의 나머지 조항에서 상충되는 조항보다 우선합니다. 의심의 여지를 없애기 위해, 본 조항 파트 B 의 나머지 부분과 전체 계약에서 EU 표준 계약 조항의 조건을 모순되지 않고 단순히 넘어서는 조항은 계속 유효합니다.

11. 책임

본 계약의 본문 내 섹션 7 을 침해하지 않는 범위 내에서, 관리자는 손해에 대해 책임을 지며 (i) 컨트롤러의 본 계약에 따른 의무 위반 및/또는 기타 해당 데이터 보호법 위반으로 인해 발생하는 제 3 자의 청구 또는 감독 당국 명령 또는 벌금의 결과를 포함한 기타 손해 및 책임에 대해 처리자를 면책해야 합니다. 및/또는 (ii) 본 계약 조항 또는 컨트롤러의 기타 지침의 적절한 실행을 기반으로 하는 한 프로세서의 해당 데이터 보호법 위반. 이는 컨트롤러가 책임을 발생시키는 상황에 대해 책임을 지지 않는 경우에는 적용되지 않습니다.

부록 1: 공동 작업의 역할, 작업 및 범위

1. B2B Connect Platform 관련 처리 활동

| 절차 | 목적/범위 | 역할 및 작업 | 데이터 범주 및 데이터 주체 |
|--------------------------------|------------------------------------|---|--|
| B2B Connect 플랫폼 서비스에 대한 시스템 지원 | ASP 직원에게 사용자 지원 제공(티케팅 도구/콜센터를 통해) | MBK: 프로세서(MBAG: 하위 처리자) 각각 ASP 에 대한 지원을 제공합니다. ASP: 컨트롤러 사용자 지원을 포함한 Web-Part 사용 | ASP 데이터: 고객 이름/회사명, 고객 직원 이름 및 고객 연락처 데이터, 고객 주소, 지원 티켓/사고 관련 정보, ISP 회사 직함, 직원 이름 또는 구매 주문 관련 데이터를 포함한 거래 및 관련 ISP 데이터를 포함한 애프터 서비스 시스템 사용 데이터에 대한 정보(필요한 경우) |

2. 비즈니스 분석

| 절차 | 목적/범위 | 역할 및 작업 | 데이터 범주 및 데이터 주체 |
|--|--|--|--|
| 디스플레이, 보고 및 분석 | B2B Connect Seller Center 에 ISP 트랜잭션 데이터 표시, 보고서 및 분석 제공 | MBK: 프로세서(MBAG: 하위 처리자) B2B Connect Seller Center 에 ISP 트랜잭션 데이터를 표시하고, ASP 요청 시 보고서 및 분석을 제공합니다. ASP: 컨트롤러 데이터 표시, 보고 및 분석을 포함한 WebPart 사용 | ISP 데이터: ISP 회사명, 사용자명, 사용자 ID, 주문 내역(주문일, 주문한 부품/서비스, 주문수량, 판매량, 미주문(매출 손실), B2B Connect Platform/A/S 관련 서비스 사용 빈도, 배송 시간), 상기 매출액을 기반으로 한 분석 및 보고서 ASP 데이터: 회사명, 사용자명, 사용자 ID |
| 캠페인 제안 서비스(MBK 및/또는 ASP; 그렇지 않으면 해당 사항 없음) | MBAG 및 MBK(해당되는 경우는)는 제공된 데이터를 사용하여 비즈니스 분석을 실행하고 MBK 및 ASP 에 대한 관련 마케팅 캠페인을 생성하고 마케팅 캠페인 운영을 지원합니다. | 엠바그: 프로세서 비즈니스 분석 데이터가 있는 데이터베이스를 호스팅합니다. MBK 및 ASP 에 제공된 데이터를 기반으로 애플리케이션을 운영하고 마케팅 캠페인을 생성하여 다양한 직접 마케팅 채널을 | ISP 데이터: ISP 회사명, 사용자명, 사용자 ID, 주소, 이메일, 전화번호, 주문내역(주문일자, 주문부품/서비스, 주문수량, 판매, 미주문(매출손실), B2B Connect Platform 사용 |

| | | | |
|--|--|--|---|
| | <p>여기에는 일반적으로 MBAG 가 다른 직접 마케팅 채널(특정 시장에서 해당되는 경우)을 통해 ISP 에 연락할 수 있도록 ISP 목록(예: 리드 포함)을 포함한 마케팅 자료를 MBK 또는 ASP 에 제공하는 것이 포함되며, 여기에는 이러한 목적을 위해 마케팅 자료 + 딜러 목록을 MBK 또는 ASP 로 전송하는 것이 포함됩니다.</p> | <p>통해 ISP 에 연락할 수 있도록 합니다. 이를 위해 마케팅 자료 + ISP 목록을 MBK 및/또는 ASP 로 전송합니다.</p> <p>MBK: 컨트롤러</p> <p>마케팅 캠페인을 위한 ISP 목록 + 마케팅 자료 수신(마케팅 캠페인은 해당되는 경우 MBK 가 단독 책임으로 운영함)</p> <p>ASP 에 유사한 서비스를 제공할 수 있음(이 경우 ASP 에 대한 프로세서 역할도 함)</p> <p>ASP: 컨트롤러</p> <p>마케팅 캠페인을 위한 ISP 목록 + 마케팅 자료 수신(마케팅 캠페인은 ASP 가 단독으로 운영함)</p> | <p>빈도/A/S 관련 서비스, 배송시간)</p> <p>ASP 데이터: 회사명, 사용자명, 아이디, 주소, 이메일, 전화번호</p> |
| <p>직접 마케팅 캠페인 서비스(ASP; 그렇지 않으면 해당 사항 없음)</p> | <p>선택적으로, ASP 가 주문하는 경우 MBK 는 ASP 가 최종 고객 연락처 데이터를 업로드하고 MBK 가 ASP 의 이름으로 ASP 를 대신하여 캠페인을 배포할 수 있는 전용 웹 서비스를 제공하여 고객에게 마케팅 자료를 보내는 것을 지원할 수 있습니다. 또한 MBK 는 MB 콜센터를 통해 ISP 에 연락하여 마케팅 지원 서비스를 통해 ASP 를 지원할 수 있습니다</p> | <p>MBK: 프로세서</p> <p>MBK 는 ASP 를 대신하여 마케팅 캠페인(이메일)을 발송할 수 있습니다(또는 MBAG 또는 해당 문제에 대해 다른 하위 처리자를 참여시킬 수 있음). 이 경우 MBK 는 ASP 가 최종 고객 데이터(이름, 이메일 주소)를 MBK 로 전송할 수 있는 인터페이스를 제공합니다.</p> <p>그런 다음 MBK 는 마케팅 이메일 발송을 위해 전송된 데이터를 처리합니다(MBK 의 제 3 자 서비스 제공업체를 통해서도 가능).</p> <p>선택적으로 MBK 는 MB 콜센터를 통해 ISP 에 연락하여 이전 비즈니스 거래에 대한 후속 조치를 취할 수 있습니다</p> <p>ASP: 컨트롤러</p> <p>마케팅 캠프 운영</p> | <p>ASP 데이터: 회사명, 사원명, 아이디, 주소, 이메일, 전화번호</p> <p>ISP 데이터: 회사명, 연락처, 사원명, 이메일, 주문내역(주문일자, 주문한 부품/서비스, 주문수량, 판매량, 미주문(매출 손실), B2B Connect Platform/A/S 관련 서비스 사용 빈도, 추가 리드 관련 정보</p> |

3. 받는 사람

각자의 관리 책임을 수행하기 위해 필요한 경우에만 개인 데이터가 공개되는 전담 역할을 가진 제한된 개인(예: HR, IT 및 재무 계약자(해당되는 경우)을 포함한 계약자) 그룹 법인, 컨설턴트, 감사, 회계사; 금융 기관; 법 집행 기관, 정부 기관, 규제 당국.

부록 2: 기술적 및 조직적 조치

다음 기술적 및 조직적 조치는 관련 환경의 개별 기능 구성 요소에서 구현된 조치를 반영합니다. 하위 기능 및 응용 프로그램에 따라 아래에 표시된 모든 조치가 완전히 구현되지 않을 수 있습니다(예: 특별히 보호되는 데이터 센터와 같이 특별히 보호된 환경에서 이미 운영되는 응용 프로그램에 대한 특별 액세스 제어 조치). 각 제품 구성 요소, 하위 기능 또는 (부분) 응용 프로그램에 대해 취해진 기술 및 조직적 조치에 대한 구체적인 자세한 설명은 요청 시 제공됩니다.

파트 A의 부록 2(하위 부록 2)를 참조하십시오.

부록 3: 하위 처리자

| # | 주소/위치를 포함한 MBK 에 대한 하위 절차 | 처리의 주제 및 성격 | 기간 |
|----|---------------------------|---------------------------|-----------------------------|
| 1. | 메르세데스-벤츠 그룹 AG | B2B 플랫폼 기술 운영 + 사용자 지원 제공 | 기간 동안 ASP 는 B2B 플랫폼을 사용합니다. |
