**개인정보 공유 부록(회사 정보)**

**개정 날짜: 2024년 3월 12일**

본 개인정보 공유 부록(이하 “DSA”)의 목적에 따라 본 DSA를 참조하는 계약 또는 기타 계약 형태(이하 “계약”)를 이행하는 Merck Sharp & Dohme LLC 법인 또는 계열사는 “회사”로 지칭하며 해당 모든 계약의 상대 당사자를 “공급업체”로 통칭한다. 회사와 공급업체는 각각 “당사자”로 지칭하며 둘을 모두 지칭하는 경우 “당사자들”로 지칭한다.

배경

1. 계약을 체결한 당사자들은 계약에 덧붙여 하나 이상의 구매 또는 작업 주문, 프로젝트 계약, 프로젝트 계획 부록, 작업 명세서, 작업 지시서 또는 기타 서비스 계약(각각 “작업 지시서”)을 체결하여 그 안에서 고려되는 서비스(이하 “데이터 공유 목적”)를 관장할 수 있다.
2. 당사자들은 계약과 관련된 모든 개인정보 공유가 데이터 보호법을 준수하여 수행되도록 보장하고 해당 데이터의 독립적 컨트롤러로서 공급업체의 역할을 명확히 하기 위해 계약 조건을 보완하기를 희망한다.

당사자들은 다음에 동의한다.

1. *개인정보 공유 활동*. 계약과 관련하여 처리되는 개인정보의 경우 해당 내용, 성격, 공유 목적 및 기간, 관련 데이터 주체의 카테고리, 개인정보의 카테고리는 “데이터 처리 세부 정보” 계약의 보조 문서에 명시되어 있다.
2. *적용 대상*. 본 DSA의 조항은 해당 작업 지시서에 달리 명시되지 않는 한 계약에 따른 모든 작업 지시서에 적용된다.
3. *공급업체의 의무*. 계약과 관련하여 개인정보를 처리할 때 공급업체는 다음을 준수해야 한다.
	1. 데이터 보호법 및 본 DSA에 따른 공급업체의 의무를 준수해야 하며, 공급업체가 이러한 의무를 이행할 수 없는 경우 공급업체는 즉시 이를 회사에 알리고 회사가 규정 위반을 해결하는 데 필요하다고 판단하는 모든 합리적이고 적절한 조치를 취해야 한다.
	2. 본 DSA 및 계약에 명시된 대로만 개인정보를 처리하되 다음의 경우는 제외한다.
		1. 공급업체가 정보 주체의 사전 동의를 얻은 경우.
		2. 특정 행정, 규제 또는 사법 절차의 맥락에서 법적 청구의 확립, 행사 또는 방어에 필요한 경우.
		3. 정보 주체 또는 다른 자연인의 중요한 이익을 보호하기 위해 필요한 경우.
		4. 적용 가능한 법률에 따라 달리 요구되는 경우, 이와 같은 경우 공급업체는 해당 법률에서 금지하지 않는 한 해당 법적 요구 사항을 회사에 알려야 하고 필요한 공개의 성격과 범위를 제한하기 위해 최선의 노력을 다해야 하며 해당 법률을 준수하는 데 필요한 최소한의 개인정보만 공개해야 한다.
	3. 제3자가 최소한 본 DSA 및 계약에 명시된 의무만큼 개인정보를 보호하는 조항이 포함된 서면 계약을 체결하지 않은 상태에서 개인정보를 제3자에게 공개하거나 이전하지 않는다.
	4. 계약에 명시되거나 본 DSA에 따라 승인된 사항을 벗어나서 개인정보를 판매, 공유, 보유, 사용 또는 공개하지 않는다.
	5. 직원, 계열사, 대리인, 하청업체 및 기타 대표자의 모든 작위 또는 부작위에 대해 전적인 책임을 진다.
	6. 합리적이고 적절한 서면 정보 보안 및 개인정보 보호 프로그램을 시행하고 유지한다. 이러한 프로그램은 계약과 관련하여 처리되는 개인정보의 성격에 상응하는 물리, 기술 및 조직 차원의 조치를 포함해야 하고 해당 조치는 모범적인 업계 관행(또는 부록 1에서 요구할 수 있는 기준보다 높은 기준)을 충족 또는 초과하며 개인 데이터 침해로부터 개인정보를 합리적으로 보호할 수 있는 조치로써 본 DSA의 요구 사항을 충족하기에 충분한 방식으로 개인정보 처리를 담당하는 모든 직원에 대한 교육, 부록 1에 설명되어 있는 조치, 부록 1에서 달리 다루지 않는 범위의 조치 및 다음과 같은 적절한 조치를 포함한다.
		1. 개인정보의 가명 처리 및 암호화
		2. 처리 시스템 및 서비스의 지속적인 기밀성, 무결성, 가용성 및 탄력성을 보장하는 능력
		3. 물리적 또는 기술적 사고가 발생한 경우 적시에 개인정보에 대한 가용성 및 액세스를 복원할 수 있는 능력
		4. 처리의 보안을 보장하기 위한 기술적, 조직적 조치의 효율성을 정기적으로 테스트, 평가 및 검토하는 프로세스
		5. 어떠한 사건이 개인정보 침해에 해당하는지 여부를 감지 후 72시간 이내에 확인할 수 있는 능력
	7. 공급업체가 관리 또는 통제하는 범위 내에서 또는 공급업체의 작위 또는 부작위로 인해 개인 데이터 침해가 실제로 발생하였거나 발생하였음이 합리적으로 의심되는 경우(“공급업체 개인 데이터 침해”) 공급업체는 다음을 수행해야 한다.
		1. 부당한 지체 없이 회사에 고지한다(모든 경우에 공급업체 개인 데이터 침해를 인지한 후 24시간 이내).
		2. 회사가 만족할 수 있는 방식으로 해당 공급업체 개인 데이터 침해의 재발을 방지하고 시정하는 데 필요한 적절한 조사와 모든 사후 처리를 수행한다.
		3. 기록 보관 및 보고와 관련된 것을 포함하여 회사가 데이터 보호법을 준수하는 데 필요하다고 판단하는 모든 정보와 공급업체 개인 데이터 침해와 관련하여 회사가 합리적으로 요청할 수 있는 기타 모든 정보를 회사에 즉시 제공한다.
		4. 개인정보가 영향을 받았을 수 있는 모든 데이터 주체에게 데이터 보호법에 따라 요구되는 내용을 포함하여 고지한다.
		5. 고지가 공급업체 또는 회사에 의해 제공되었는지 여부와 관계없이 데이터 주체에 대한 고지에 관하여 일방 당사자의 비용 및 지출에 대한 전적인 책임을 진다.
	8. 다음 사건 발생 시 모든 경우에 부당한 지체 없이 24시간 내에 빠르게 회사에 고지한다.
		1. 계약과 관련된 개인정보와 연관이 있는 관할 데이터 보호 또는 기타 규제 당국의 불만 사항, 문의, 요청 또는 우려 사항
		2. 개인정보 액세스(개인정보의 처리에 관한 정보 요청 포함), 정정, 수정, 교정, 공유, 삭제 또는 처리 중단 등 데이터 보호법이나 회사 또는 공급업체의 개인정보 보호 정책에 따른 권리 행사 요청을 비롯하여 계약과 관련하여 개인정보와 연관된 데이터 주체의 불만 사항, 문의, 요청 또는 우려 사항
	9. 공급업체와 회사가 데이터 보호법 및 본 DSA에 따른 각자의 의무를 준수하는 데 필요하여 회사에서 요구하는 모든 합리적이고 적절한 조치를 수행한다.
	10. 적용 가능한 법률에서 달리 요구하는 경우를 제외하고 데이터 공유 목적을 달성하는 데 필요한 기간 이상 개인정보를 보관하지 않는다.
	11. 공급업체가 해당 개인정보를 받은 형식과 동일하게 회사가 공유한 개인정보의 정확성과 무결성을 유지한다.
	12. 개인정보가 해당 고지, 동의, 허가 및 권리에 따라서만 처리되었으며 본 DSA에서 허용되는 바에 따라 그리고 각 회사 및 공급업체가 데이터 보호법을 준수하는 방식으로 개인정보가 처리되었음을 입증하는 데 필요한 모든 기록을 유지한다.
	13. 공급업체가 개인정보의 국경 간 이전을 제한하는 국가 또는 지역의 데이터 주체에 관한 개인정보를 처리하는 경우, 공급업체는 데이터 보호법을 준수하여 처리해야 하며 이는 표준 계약 조항 또는 이와 유사한 개인정보 이전 보호 메커니즘의 체결을 포함할 수 있다.
	14. 더 높은 수준의 산업 표준 또는 데이터 보호법을 준수하기 위해 변경 사항을 적용하는 경우를 제외하고 회사가 계약 관련 관행에 대해 가장 최근 실시한 실사와 관련하여 회사에 공개된 공급업체의 프라이버시 및 데이터 보안 관행을 실제적으로 일관되게 적용해야 한다. 단, 공급업체는 이전에 공개된 관행을 저하하는 프라이버시 및 데이터 보안 관행을 나중에 공개하여 해당 관행의 표준을 축소할 수 없다. 공급업체는 해당 실사에서 공급업체가 제공한 모든 응답이 사실이고 정확하고 완전하며, 공급업체의 승인된 대리인이 해당 실사를 완료했음을 진술 및 보장한다. 공급업체는 공급업체의 개인정보 보호 및 데이터 보안 관행에 대한 모든 중요한 변경 사항을 즉시 회사에 알려야 한다.
	15. 데이터 보호법에 의해 요구되는 경우 개인정보 보호 담당자를 지정하고 담당자의 이름, 전화번호를 회사에 알린다.
	16. 공급업체는 본 DSA를 체결함으로써 DSA에 명시된 제한 사항의 이해 및 준수를 확인한다는 사실을 인정하고 이에 동의한다.
4. *면책.* 계약 등에 따른 회사의 권한이나 권리 또는 공급업체의 의무를 제한하지 않고 당사자들은 계약과 관련하여 공급업체가 처리하는 개인정보와 관련된 공급업체 개인 데이터 침해로 인하여 회사 및 그 계열사와 각각의 임원, 이사, 직원, 계약자, 임시 직원, 하청업체, 대리인 및 기타 대표자(이하 각 “면책 당사자”)에게 발생한 손실, 손해, 벌금, 비용 또는 지출(법적 비용 및 지출 포함)에 대해 공급업체가 면책 당사자를 면책하는 데 동의한다. 본 장에 따른 모든 책임에는 계약에 따라 적용 가능한 책임 제한 또는 배제가 적용되나 해당 책임이 공급업체의 과실 또는 고의적인 부정 행위의 결과인 경우에는 그렇지 아니하다.
5. *정의*
	1. “데이터 보호법”은 유럽 연합 일반 데이터 보호 규칙(EU General Data Protection Regulation) 및 이와 관련된 국내이행입법, 건강보험의 이전 및 책임에 관한 법(Health Insurance Portability and Accountability Act), 캘리포니아주 프라이버시 권리법(California Privacy Rights Act) 및 기타 국가, 주, 연방, 지방 또는 지역의 데이터 보호, 데이터 보안 또는 프라이버시 법을 비롯하여 적용 가능한 모든 데이터 보호, 데이터 보안 또는 프라이버시 법을 의미한다.
	2. “개인정보”는 개인을 식별하거나 개인을 식별, 위치 파악, 추적 또는 연락하는 데 사용될 수 있는 데이터를 비롯하여 식별되거나 식별 가능한 개인과 관련하여 계약과 연관된 모든 데이터를 의미한다. 개인정보에는 이름, 신분증 번호 또는 고유한 직책 등 직접 식별 가능한 정보와 생년월일, 고유한 모바일 또는 웨어러블 기기 식별자, 세대를 식별하는 데 사용될 수 있는 정보, 전화번호, 키 코딩된 데이터, IP 주소와 같은 온라인 식별자, 개인 활동, 행동, 선호 등 간접 식별 가능한 정보가 포함되며 데이터 보호법에 따라 “개인 데이터”를 구성하는 모든 데이터가 포함된다.
	3. “처리”는 수집, 기록, 구성, 구조화, 저장, 액세스, 조정 또는 변경, 검색, 참조, 사용, 전송이나 배포 또는 기타 방식에 의한 공개, 평가, 분석, 보고, 공유, 정리 또는 조합, 제한, 삭제, 파기 등 방식의 자동화 여부와 관계없이 개인정보 또는 일련의 개인정보에 대해 작업 또는 일련의 작업을 수행하는 것을 의미한다.
	4. “개인 데이터 침해”는 전송, 저장 등 처리된 개인정보의 우발적 또는 불법적인 파기, 손실, 변경, 무단 공개 또는 액세스를 의미한다.
	5. “표준 계약 조항”(Standard Contractual Clauses)은 유럽 위원회(European Commission)가 개인 데이터에 대한 적절한 수준의 보호를 제공하는 것으로 평가하지 않은 제3국으로의 개인 데이터 이전에 관한 표준 계약 조항을 의미한다. 이는 유럽 위원회가 2021년 6월 4일 공개하였으며, 수시로 업데이트될 수 있다.
	6. 상술된 정의가 데이터 보호법 내 관련 정의의 범위를 제한하거나 축소하는 경우 위 정의는 해당 데이터 보호법의 정의와 일치하도록 확장된다.
	7. 본 장에 정의 규정이 없는 경우, 용어는 적용 가능한 모든 데이터 보호법을 준수하는 방식으로 해석된다.
6. *해석*.
	1. 정의된 용어로서 본 DSA에 사용되었지만 여기에 정의되지 않은 용어는 본 계약의 다른 부분에 명시된 의미를 갖는다.
	2. “포함하다” 및 “포함”이라는 단어는 제한 없이 포함한다는 의미로 해석된다.
	3. 서비스 계약 및 이 DSA에 따른 의무를 이행함에 있어, 양 당사자는 MSD 및 그 계열사의 기업 정책이 EU 일반 데이터 보호 규정을 포함한 해당 데이터 보호 법률의 문자 및 정신 내에서 MSD의 비즈니스가 수행될 것을 요구한다는 점을 인정합니다. 양 당사자가 동일한 데이터 보호 법률의 적용을 받지 않는 경우, 양 당사자가 그러한 법률에 포함된 모든 관련 데이터 보호 기준을 준수할 것으로 예상됩니다.
	4. 본 계약에 따른 데이터 공유 목적과 관련하여 공급업체는 하나 이상의 회사 계열사의 개인정보를 처리할 수 있다. 그러한 경우, 해당 계열사가 계약 또는 본 DSA의 당사자로 지정되었는지 여부와 관계없이 해당 회사 계열사는 개인정보의 “컨트롤러”이자 본 DSA의 제3자 수혜자로 간주되며 본 DSA에 따라 회사에 부여된 모든 권리와 보호에 의존하고 이를 집행할 자격이 있다.
	5. 본 DSA는 계약에 통합되어 계약의 일부를 구성한다.
	6. 계약 조항과 본 DSA 조항 사이에 충돌이 발생하는 경우 본 DSA의 조항이 우선한다. 단, 계약 조항이 계약과 관련하여 처리되는 개인정보를 더 높은 수준으로 보호하는 경우에는 보호 수준이 더 높은 해당 계약 조항이 우선한다.
	7. 본 DSA의 조항과 표준 계약 조항 사이에 충돌이 발생하는 경우 표준 계약 조항의 규정이 우선한다.
	8. 여기에 명시적으로 개정된 경우를 제외하고 계약 조항은 완전한 효력을 유지한다.
	9. 본 DSA가 영어와 외국어로 작성되고 영어 텍스트와 외국어 텍스트 사이에 차이가 있는 경우 영어 텍스트가 우선한다.
	10. 본 DSA의 장 및 기타 제목은 참조의 편의를 위한 것일 뿐이며 본 DSA의 의미나 해석의 일부를 구성하거나 이에 영향을 미치지 않는다.
	11. 본 DSA의 첨부 자료 및 부록은 본 DSA 내에 명시적으로 규정된 것과 같은 수준으로 본 DSA의 일부를 구성하는 것으로 간주된다.
	12. 본 DSA의 규정은 분리 가능하다. 문구, 조항 또는 규정의 전체 또는 일부가 유효하지 않거나 시행 불가능한 경우, 그러한 무효 또는 시행 불가능성은 해당 문구, 조항 또는 규정에만 영향을 미치며 본 DSA의 나머지 부분은 완전한 효력을 유지한다.
	13. 본 DSA는 회사와 공급업체가 특정 데이터 공유 목적에 적용되는 다른 DSA를 체결한 경우를 제외하고 데이터 공유 목적과 관련된 모든 개인정보의 처리를 관장하며 데이터 공유 목적에 적용되는 계약 조항을 보완한다.
	14. 본 DSA는 동일한 여러 개의 사본이 허용되며 각 사본은 모두 함께 하나의 동일한 계약을 구성한다. 어떠한 당사자든 이러한 사본에 서명∙날인함으로써 본 DSA를 체결할 수 있다.
	15. 본 DSA는 본 DSA의 주제와 관련하여 당사자 간의 완전한 합의를 구성하며 (법이 허용하는 한도 내에서) 해당 주제와 관련하여 당사자 간의 모든 이전 진술이나 구두 또는 서면 합의를 대체한다. 단, 본 DSA의 어떠한 내용이나 당사자의 어느 일방도 허위 진술에 대한 책임을 배제하려고 시도하지 않는다.
	16. 계약의 준거법과 관할권 규정은 본 DSA에 적용된다.
7. *업데이트 제한*.
	1. 당사자들이 계약을 갱신, 수정, 새로운 업무 명세서를 발행하거나, 계약이나 계약 하의 어떠한 업무 명세서를 어떠한 방식으로든 수정하는 경우(“발동 이벤트”), <https://www.msdprivacy.com/privacyterms/>에 위치한 “Data Sharing Addendum (Company Data)” 하의 가장 최근 문서가 다음 발동 이벤트까지 이 DSA의 조건을 대체하고 대신하게 되며, 발동 이벤트 발생 후 30일 이내에 이의가 제기되지 않는 한 그러합니다. 그럼에도 불구하고, 새로운 적용 가능한 데이터 보호 법률, 판례, 또는 관련 데이터 보호 당국이 발행한 지침을 준수하기 위해 필요한 것으로 한정된 새로운 조항이나 수정된 조항을 확보한 후 선의로만 이루어질 수 있는 이 DSA의 조건에 즉각적인 수정이 필요한 상황이 있을 수 있으며, 이는 오직 7(b)에서 명시된 이유로만 발생합니다.
	2. 다음 시나리오 중 하나가 발생하는 경우, 당사자들은 상기 주소에 게시된 최신 조항에 즉시 동의하게 되며, 회사가 privacy\_updates@msd.com에서 통지를 받기를 요청한 모든 단체에 새로운 조항을 통보한 후 30일 이내에 이의가 제기되지 않는 한 그러합니다.

		1. 적용 가능한 데이터 보호 법률이 기존 DSA의 계약 조건이 업데이트된 법률의 요구 사항을 충족시키기에 부적합하게 업데이트된 경우,
		2. 적용 가능한 데이터 보호 법률에 변경이 있고 당사자들이 법률 변경으로 인해 이 조항들을 수정할 합리적이고 정당한 이익이 있는 경우, 예를 들어 제한 없이 더 이상 필요하지 않은 요구 사항을 제거하는 경우 등,
		3. (i) 또는 (ii) 위에서 설명한 법률 변경과 유사한 효과를 가진 관련 데이터 보호 당국이 발행한 새로운 판례 또는 지침이 있는 경우.
8. *부록의 적용 가능성.* 여기에 부록 2로 첨부된 표준 계약 조항과 부록 3으로 첨부된 첨부 자료는 적용 가능한 데이터 보호법에서 요구하는 한도까지만 적용된다. 당사자들은 각 관할권에서 적용 가능한 데이터 보호법의 요구 사항에 부합하는 범위 내에서 이에 따라 필요한 수준으로만 이러한 조항과 첨부 자료를 준수하는 데 동의한다.
9. *고지.* 본 DSA에 따라 제공되는 고지(각 “고지”)는 서면으로 이루어져야 한다. 본 DSA에 따라 제공되는 고지는 적용 가능한 계약의 고지 규정에 부합하는 방식으로 이루어져야 하며 이와 함께 이메일을 통해 사본을 msd\_privacy\_office@msd.com으로 발송하되 제목란에 “공급업체의 DSA 고지” 또는 개인 데이터 침해의 경우 “긴급: 개인 데이터 침해 고지”를 입력한다.

**부록 1 – 정보 기술 보안 조치**

1. 정의 - 이 전시에서 사용되는 각각의 정의된 용어는 아래에 주어진 그 용어에 대한 정의를 가집니다. 이 전시에서 사용되지만 여기서 정의되지 않은 정의된 용어는 계약의 다른 부분에서 명시된 의미를 가집니다.
	1. “회사 정보”란 서비스와 관련하여 공급자 또는 공급자의 제3자 서비스 제공자에게 제공되거나, 획득되거나, 생성되거나, 처리되는 회사 또는 회사의 제휴사 또는 각각의 공급자, 고객 또는 기타 사업 파트너의 정보와 계약에 따라 기밀로 취급되어야 하는 모든 기타 정보를 의미합니다.
	2. “데이터 유출”이란 회사 정보에 대한 실수 또는 무단 파괴, 손실, 변경, 사용, 전송 또는 공개 또는 접근을 의미합니다.
	3. “엔드포인트”란 공급자 시스템의 컴퓨터, 노트북 또는 데스크톱, 모바일 장치, 실험실 장비, 서버 또는 기타 장치를 포함하며, 외부 제3자 사이트(예: 클라우드 제공자)에서 호스팅되는 것을 포함합니다.
	4. “통지 이벤트”란 모든 법률에 따라 개인 또는 엔티티에게 통지를 요구하는 이벤트, 데이터 유출을 포함하여 의미합니다.
	5. “보안 이벤트”란 (A) 데이터 유출, (B) 통지 이벤트, (C) 공급자 시스템의 운영에 대한 무단 접근 또는 방해, 또는 (D) 이 전시, 계약 또는 어떤 법률에 따른 공급자의 보안 의무 위반을 의미합니다.
	6. “주제 소프트웨어”란 서비스와 관련하여 제공되거나 사용되는 모든 소프트웨어를 의미하며, 회사 또는 회사의 제휴사의 정보 시스템의 컴퓨터, 노트북 또는 데스크톱, 모바일 장치, 실험실 장비, 서버, 기타 장치 또는 기타 구성 요소에 전달되거나 설치되는 모든 소프트웨어를 포함합니다.
	7. “공급자 시스템”이란 공급자의 네트워크와 모든 시스템, 주제 소프트웨어를 포함하여, (A) 서비스와 관련하여 제공되거나 사용되는, (B) 회사 정보 또는 회사 또는 그 제휴사를 위한 결과물 또는 진행 중인 작업이 저장되거나 그 외에 처리되거나 접근되는, (C) 회사 또는 그 제휴사의 정보, 네트워크 또는 기타 시스템에 연결되거나 회사 또는 그 제휴사의 정보, 네트워크 또는 기타 시스템에 접근할 수 있는, 또는 (D) 위의 어떤 것에도 연결되거나 위의 어떤 것에도 접근할 수 있는 것을 의미합니다.
2. 네트워크 보안 - 공급자는 네트워크 보안 정책, 절차 및 통제를 유지하고, 공급자의 업계에서의 모범 사례에 따라 네트워크 보안 활동을 수행해야 하며, 이는 최소한 네트워크 방화벽 프로비저닝, 침입 탐지 및 방지 통제, 분산 서비스 거부 공격(DDoS) 보호 통제 및 취약성 평가 및 침투 테스트를 정기적으로 수행하는 것을 포함합니다(하지만 공급자의 업계에서의 모범 사례에 따라 연간 이하로는 안됩니다). 어떤 경우에도 공급자의 네트워크 보안 정책, 절차 또는 통제는 회사 정보와 공급자 시스템의 보호에 적용되는 것이 공급자가 자신의 정보와 유사한 성격의 기타 시스템의 보호에 적용하는 것보다 덜 엄격하고 보호적이어서는 안됩니다.
3. 응용 프로그램 보안 - 제공되는 서비스의 성격에 따라 적용되는 경우, 공급자는 공급자 소프트웨어의 개발 및 변경을 관리하는 소프트웨어 개발 수명주기 프로세스 및 제어("SDLC 프로세스")를 가져야 합니다. 이에는 업데이트, 업그레이드, 패치, 개선, 버그 수정, 수정, 개선, 수정, 개정, 릴리스 및 기타 변경 사항이 포함됩니다. SDLC 프로세스는 최소한으로 인정되고 비교 가능한 업계 표준 보안 소프트웨어 개발 방법론을 포함해야 합니다. 공급자는 공급자 정보 시스템이 적절한 보안 및 기능성으로 최신 상태를 유지하도록 패치 관리 프로세스를 따라야 합니다. 공급자는 공급자 정책 및 절차에서 제공된 시간 내에 위험에 따라 적절하게, 식별된 취약점을 시정하고 재테스트해야 합니다.
4. 데이터 보안 - 제공되는 서비스의 성격에 따라 적용되는 경우, 공급자는 회사 정보를 인정되고 비교 가능한 업계 관행 및 표준에 따라 처리, 저장, 그리고 그 외의 방식으로 처리해야 합니다. 이는 11항(해당하는 경우 PCI DSS 포함)에 명시된 것과 모든 법률에 따라야 합니다. 공급자는 데이터 유출에 대한 합리적인 보호 조치를 설정하고 유지해야 합니다. 공급자의 기타 의무를 제한하지 않고, 공급자는 모든 회사 정보를 공급자 업계의 모범 사례에 따라 저장하고, 모든 법률을 준수하며, 암호화 및 방화벽을 포함한 공급자 업계의 모범 사례를 충족하는 보안 조치를 사용하여 회사 정보를 데이터 유출로부터 보호해야 합니다. 공급자가 회사 정보를 오프사이트 시설에 저장하는 경우, 공급자는 계약 또는 계약과 관련하여 체결된 모든 계약의 모든 조건을 준수해야 하며, 제삼자에게 회사 정보를 공개하거나 제삼자가 제품 또는 서비스를 제공하거나 돕는 것과 관련하여, 공급자는 회사가 합리적으로 수용할 수 있는 오프사이트 저장 시설을 사용해야 합니다. 이는 앞서 언급한 것을 제한하지 않고, 이 전시회의 모든 규정을 완전히 준수해야 합니다. 또한, 이러한 오프사이트 저장 시설의 제공자는 공급자와 해당 제공자 사이의 서면 비밀 유지 계약에 의해 구속되어야 하며, 이 계약은 계약 또는 계약과 관련하여 체결된 모든 계약보다 엄격하지 않은 조건을 포함하고 있어야 하며, 이를 통해 저장된 모든 회사 정보를 보호해야 합니다.
5. 데이터 저장 - 제공되는 서비스의 성격에 따라 적용되는 경우, 모든 회사 정보는 공급자의 지정된 컴퓨팅 및 저장 자원에서만 처리, 저장 및 그 외의 방식으로 처리됩니다. 회사 정보는 노트북 또는 모바일 장치에서만 처리, 저장 또는 그 외의 방식으로 처리되거나 이동되며, (A) 공급자의 노트북 또는 모바일 장치인 경우, (B) 공급자가 해당 노트북 또는 모바일 장치에 있는 모든 회사 정보를 아래 7항의 암호화 표준에 따라 암호화하고, (C) 해당 노트북 또는 모바일 장치가 11항에 명시된 것과 같은 인정되고 비교 가능한 업계 관행 및 표준에 따른 엔드포인트 제어를 받는 경우에만 가능합니다. 회사 정보는 바로 위의 문장에서 제공된 것 외에는 휴대용 장치에서 처리, 저장 또는 그 외의 방식으로 처리되지 않습니다. 공급자는 지정된 백업 및 복구 프로세스의 일부로 회사 정보의 모든 백업을 저장해야 하며, 이러한 회사 정보의 백업은 이 전시회, 이 5항 및 아래 7항의 요구 사항에 따라 암호화되어야 합니다.
6. 데이터 전송 - 제공되는 서비스의 성격에 따라 적용되는 경우, 회사 정보의 전자적 전송 또는 교환은 안전한 수단(HTTPS 또는 SFTP 또는 동등한 것을 사용)을 통해 이루어져야 하며, 이는 11항에 명시된 것과 같은 인정된 비교 가능한 산업 표준과 일치하며, 오직 아래의 7항에 따라 이루어져야 합니다.
7. 데이터 암호화 - 제공되는 서비스의 성격에 따라 적용되는 경우, 공급자의 기타 의무를 제한하지 않고 추가로, 공급자는 어떠한 법률에 따라 보호를 받아야 하는 개인 정보 또는 당시의 결제 카드 산업 데이터 보호 표준에 따라 보호를 받아야 하는 정보를 포함하는 모든 회사 정보, 백업 데이터를 포함하여, 상업적으로 지원되는 암호화 솔루션을 사용하여 암호화된 형태로 보관해야 합니다. 공급자는 11항에 명시된 것과 같은 인정된 비교 가능한 산업 표준에 따라 회사 정보를 암호화하는 암호화 솔루션을 배포해야 하며, 대칭 암호화에 대해서는 128비트 이상의 키, 비대칭 암호화에 대해서는 2048(또는 그 이상) 비트의 키 길이를 사용해야 합니다.
8. 데이터 재사용 - 제공되는 서비스의 성격에 따라 적용되는 경우, 공급자는 모든 회사 정보를 서비스 수행을 위한 목적으로만 사용해야 합니다. 공급자는 회사 정보를 다른 애플리케이션, 환경 또는 공급자의 비즈니스 유닛에 배포, 재사용 또는 공유해서는 안됩니다.
9. 계약 종료 시 데이터 처리 - 제공되는 서비스의 성격에 따라 적용되는 경우, 공급자의 기타 의무를 제한하지 않고 추가로, 회사의 요청에 따라, 또는 계약에서 다르게 규정되지 않는 한, 계약의 만료 또는 조기 종료 시, 공급자 또는 공급자의 제휴사, 하청업체, 서비스 제공자, 대리인 또는 기타 컨설턴트가 보유하거나 통제하는 모든 회사 정보는 회사가 선택하는 대로 파기하거나 반환해야 합니다.
10. 보안 위반 통보 - 공급자의 기타 의무를 제한하지 않고 추가로, 공급자는 실제 또는 합리적으로 의심되는 보안 이벤트에 대해 알게 된 후 24시간 이내에 회사에 통보해야 합니다. 공급자는 전화(+1-704-345-6700 – 옵션 1 선택)와 이메일 Global Operations Center globalopscnt@merck.com을 통해 회사의 보안 팀에게 실제 또는 합리적으로 의심되는 보안 이벤트에 대해 통보해야 합니다. 공급자는 보안 이벤트에 대해 회사가 합리적으로 요청할 수 있는 정보와 지원을 제공해야 합니다, 이는 근본 원인 정보를 포함합니다.
11. 산업 표준 - 일반적으로 인정되는 산업 표준에는 다음과 같은 현재의 표준과 벤치마크를 설정하고 유지하는 것이 포함되지만 이에 국한되지 않습니다:
	1. 인터넷 보안 센터 - [http://www.cisecurity.org](http://www.cisecurity.org/) 참조
	2. 결제 카드 산업 / 데이터 보안 표준 (PCI/DSS) – <http://www.pcisecuritystandards.org/> 참조
	3. 국립 표준 기술 연구소 - [http://csrc.nist.gov](http://csrc.nist.gov/) 참조
	4. 연방 정보 보안 관리법 (FISMA) - [http://csrc.nist.gov](http://csrc.nist.gov/) 참조
	5. ISO/IEC 27000 시리즈 - <http://www.iso27001security.com/> 참조
	6. 구조화된 정보 표준의 발전을 위한 조직 (OASIS) – <http://www.oasis-open.org/> 참조
	7. 오픈 웹 애플리케이션 보안 프로젝트 (OWASP) – [http://www.owasp.org](http://www.owasp.org/) 참조
	8. CWE (Common Weakness Enumeration) - [http://cwe.mitre.org](http://cwe.mitre.org/) 또는 CWE/SANS Top 25 프로그래밍 오류 - <http://cwe.mitre.org/top25/> 참조
	9. SANS Institute - [http://www.sans.org](http://www.sans.org/) 참조
	10. 가장 위험한 소프트웨어 오류 <http://www.sans.org/top25-programming-errors/> 참조

회사의 합리적인 요청에 따라, 공급자는 회사가 위에 나열된 요구사항에 대한 공급자의 준수를 감사할 수 있도록 허용해야 합니다. 공급자는 가능한 한 빨리 요구사항을 준수하지 못하는 경우를 수정해야 합니다.

**부록 2**

회사가 표준 계약 조항의 모듈 1을 요구하는 방식으로 개인정보를 수출하는 경우 다음 조항이 적용된다.

*2021년 6월 4일자 위원회 시행 결정(EU) 2021/914에 첨부된 표준 계약 조항의 모듈 1(컨트롤러에서 컨트롤러로)의 본문 텍스트는 여기에 참조로 포함된다. 선택적 측면은 아래에 설명되어 있다.*

1. *제7항(도킹 조항)이 생략된다.*
2. *제11항의 경우 선택 사항 텍스트가 생략된다.*
3. *제17항의 경우 옵션 1이 선택되며 회원국은 네덜란드이다.*
4. *제18항의 경우 선택되는 관할권은 네덜란드이다.*

**부록 2의 첨부 자료 1**

**A. 당사자 목록**

*계약 보기*

**B. 양도에 대한 설명**

*“데이터 처리 세부 정보”라는 제목의 계약서 보조 문서를 참고한다.*

**C. 관할 감독 당국**

****Commission Nationale de l'Informatique et des Libertés - CNIL****
3 Place de Fontenoy

TSA 80715

75334 PARIS CEDEX 07
Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00
Website: [**http://www.cnil.fr/**](http://www.cnil.fr/)

**부록 2의 첨부 자료 2 – 기술 및 조직적 조치**

본 조항이 첨부된 DSA의 부록 1을 참고한다. 또한 데이터 수입업체는 모든 개인 데이터가 적절한 경우 가명화되고 암호화되도록 해야 한다. 또한 본 조항의 대상이 되는 개인 데이터와 관련하여 정부 기관으로부터 요청을 받을 경우 데이터 수입업체와 그 계열사는 부록 1B에 설명된 개인 데이터에 대한 (i) 미국 또는 기타 지역의 정보 기관 또는 유사한 기관의 액세스 요구 및 (ii) “공개 의무”에 대하여 추출 전에 해당 법률 및 규정에 따라 이의를 제기할 것임을 보증한다.

**부록 3**

**추가적인 주, 국가, 지역 및 지방의 법적 요구 사항**

**영국 부록: 데이터 보호법 2018 (Data Protection Act 2018)**

본 부록 3에는 2022년 3월 21일 발효된 EU 위원회 표준 계약 조항의 국제 데이터 이전 부록(International Data Transfer Addendum to the EU Commission Standard Contractual Clauses) B1.0 버전이 참조로 포함되어 있다. 부록 3은 DSA에 따라 적용 가능한 모든 이전을 포괄하고 모든 2부 필수 조항(Part 2 Mandatory Clauses)을 포함하여 계약의 모든 당사자가 완전히 실행한 것으로 간주한다.

**스위스 부록: FADP**

1. 부록 2에 설명된 데이터 이전에 FADP가 적용되는 경우, GDPR에 대한 언급은 스위스 데이터 보호법(Swiss Federal Act on Data Protection, 이하 “FADP”)에 대한 언급으로 이해되어야 한다.
2. FADP에서 요구하는 기간 동안 법인의 개인 데이터는 데이터 주체가 개인인 것과 동일한 방식으로 본 조항에 따라 보호된다.
3. 제13항: 병행 감독
	1. 데이터 이전이 FADP에 의해 관리되는 경우: 연방 데이터 보호 및 정보 위원회(Federal Data Protection and Information Commissioner, 이하 “FDPIC”)가 관할 감독 기관이다.
	2. 데이터 이전이 GDPR에 의해 관리되는 경우: 제13(a)항의 기준이 적용된다.
4. 제18(c)항: 관할권 선택: 스위스에 상거소를 두고 있는 데이터 주체는 스위스 법원에서 데이터 수출업체 및/또는 데이터 수입업체를 상대로 법적 소송을 제기할 수도 있다.

**캐나다 부록: 퀘벡법 25 (Quebec Law 25)**

* + - 1. 개인 데이터 위반과 관련하여 본 DSA에 따라 요구되는 모든 고지 및 계약에 따라 요구되는 유사한 고지는 공급업체가 본 DSA를 위반하거나 위반하려고 시도하는 경우에도 필요하다.
			2. 본 DSA의 조항과 관련하여 동의를 수집해야 하는 경우 공급업체는 계약 종료 후 3년 동안 모든 동의의 증거 또한 보관해야 한다.

**아랍에미리트 부칙: 개인 데이터 보호에 관한 연방법 제45호 (2021년)**

1. 부록 2에 설명된 데이터 전송이 아랍에미리트의 개인 데이터 보호에 관한 연방법 제45호(“PDPL”)의 적용을 받는 한, 아랍에미리트 데이터 오피스가 아랍에미리트 외부로 개인 정보를 전송하는 것을 합법화하기 위해 독자적인 표준 계약 조항을 발행하고, 당사자들이 그러한 표준 계약 조항을 체결하기 전까지, 당사자들은 부록 2에 첨부된 표준 계약 조항이 개인 정보 및 데이터 주체를 위한 적절한 보호 조치를 제공하기 위해 관련 전송에 대해 mutatis mutandis로 적용될 것에 동의합니다. 이를 위해: a. “EU 규정 2016/679”, “2016년 4월 27일 유럽 의회 및 이사회의 규정(EU) 2016/679(일반 데이터 보호 규정)” 및 “그 규정”에 대한 언급은 모두 “PDPL”로 대체됩니다. b. "EU 규정 2016/679"의 특정 조항에 대한 언급은 PDPL의 해당 조항 또는 섹션으로 대체됩니다. c. “유럽연합”, “연합”, “EU”, “EU 회원국”, “회원국” 및 “EU 또는 회원국”에 대한 언급은 모두 “아랍에미리트”로 대체됩니다. d. “관할 감독 기관” 및 “감독 기관”은 모두 “데이터 오피스”로 대체됩니다. e. 표준 계약 조항에서 발생하는 모든 분쟁은 아랍에미리트 법률에 따라 규율되며, 아랍에미리트 법원에서 해결됩니다. 당사자들은 그러한 법원의 관할권에 복종하는 데 동의합니다. f. PDPL과 부록 2에 첨부된 표준 계약 조항 간에 불일치나 충돌이 있는 경우, PDPL이 적용됩니다. g. 부록 2에 첨부된 표준 계약 조항의 의미가 아랍에미리트 외부로의 개인 정보 전송에 적용되는 한 명확하지 않거나 여러 가지 의미가 있는 경우, PDPL에 가장 부합하는 의미가 적용됩니다.
2. 아랍에미리트 데이터 오피스가 아랍에미리트 외부로 개인 정보를 전송하는 것을 합법화하기 위한 독자적인 표준 계약 조항을 발행하는 경우, 당사자들은 표준 계약 조항을 가능한 한 빨리 합의하고 구현할 목적으로 성실하게 협상할 것입니다. 앞 문장에 따라 당사자들이 표준 계약 조항을 체결한 경우, 그러한 표준 계약 조항은 PDPL이 적용되는 아랍에미리트 외부로의 개인 정보 전송과 관련하여 부록 2에 첨부된 표준 계약 조항을 대체하여, 전송과 관련하여 개인 정보 및 데이터 주체에 대한 적절한 보호 조치를 제공하기 위해 구현된 적절한 보호 조치가 됩니다.
3. 데이터 오피스가 표준 계약 조항이 적용되는 개인 정보 전송을 포괄하는 적정성 결정을 채택하거나 회사가 전송과 관련하여 다른 적절한 보호 조치가 적용된다고 판단하는 경우, 회사는 서면 통지를 통해 부록 2에 첨부된 표준 계약 조항에 구속되지 않겠다는 동의를 철회할 수 있습니다. 앞 문장에 따라 회사가 통지를 제공한 날로부터 부록 2에 첨부된 표준 계약 조항은 아랍에미리트 외부로의 PDPL이 적용되는 개인 정보 전송에 더 이상 적용되지 않습니다.

**브라질 추가 조항: LGPD - 표준 계약 조항**

브라질 일반 데이터 보호법(Lei Geral de Proteção de Dados – “LGPD”)에 따른 브라질 표준 계약 조항("SCCs")은 브라질 거주자의 데이터가 처리되는 경우 또는 데이터 전송이 필요할 경우 준수해야 합니다. 당사자들은 브라질 국가 데이터 보호 당국("ANPD")에서 발행한 SCCs를 조항에서 명시적으로 허용된 조건에 따라 수정되지 않는 한 전체적으로 채택하기로 동의합니다. 이러한 SCCs는 계약에 참조로 포함되며, 여러 텍스트 옵션이 제시된 경우 다음과 같이 선택됩니다:

섹션 3.1에 대해 옵션 B가 선택되었습니다. 수입자는 아래에 설명된 경우와 제18조의 규정에 따라 이러한 조항이 적용되는 국제 데이터 전송의 주체인 개인 데이터를 전송할 수 있습니다.

섹션 4.1에 대해 옵션 A가 선택되었습니다. 상호 지원의 의무와 당사자들의 일반 의무를 해치지 않고, 아래 지정된 당사자가 본 조항에서 규정한 의무를 주로 준수할 책임을 집니다.

a) 제14조에 따라 제공된 문서 공개 책임자:

[x] 수출자 [ ] 수입자

b) 제15조에서 다루는 데이터 주체 요청에 응답할 책임자:

[x] 수출자 [ ] 수입자

c) 제16조에서 규정된 보안 사고 통지 책임자:

[x] 수출자 [ ] 수입자

**사우디아라비아 추가 조항: PDPL - 표준 계약 조항**

개인 데이터 보호법("PDPL")에 따른 사우디아라비아 표준 계약 조항("SCCs")은 사우디아라비아 거주자의 데이터가 처리되는 경우, 데이터 전송이 사우디 관할권에 속하는 경우 또는 사우디 법이 사우디 SCCs 준수를 요구하는 경우 적용됩니다. 부록 2에 설명된 템플릿 유형과 일치하는 SCCs 버전이 완전하게 적용되며 계약에 참조로 포함됩니다.