**공동 개인정보처리자 부록**

**개정 날짜: 2024년 3월 12일**

본 공동 게인정보처리자 부록(이하 “JCA”)의 목적에 따라 본 JCA를 참조하는 계약 또는 기타 계약 형태(“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 “공동 목적”)를 관장할 수 있다.
2. 당사자들은 계약과 관련된 모든 개인정보 공유가 데이터 보호법을 준수하여 수행되도록 보장하고 해당 데이터의 공동 컨트롤러로서 당사자들의 역할을 명확히 하기 위해 계약 조건을 보완하기를 희망한다.

당사자들은 다음에 동의한다.

1. *공동 처리 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 JCA의 조항은 해당 작업 지시서에 달리 명시되지 않는 한 계약에 따른 모든 작업 지시서에 적용된다.
3. *의무*. 계약과 관련하여 처리되는 개인정보에 대해 당사자들은 다음을 준수해야 한다.
   1. 데이터 보호법 및 본 JCA에 따른 각자의 의무를 준수하며, 일방 당사자가 이러한 의무를 이행할 수 없는 경우 즉시 상대방 당사자에게 알리고 위반 사항을 해결하는 데 필요한 모든 합리적이고 적절한 조치를 취한다.
   2. 본 JCA 및 계약에 명시된 대로만 개인정보를 처리한다. 단, 상대방 당사자의 서면 동의가 있는 경우로서 다음과 같은 경우는 제외한다.
      1. 해당 당사자가 관련 데이터 보호법에 따라 데이터 주체의 유효한 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. 관련 법률에 따라 달리 요구되는 경우, 이와 같은 경우 해당 당사자는 관련 법률에서 금지하지 않는 한 해당 법적 요구 사항을 상대방 당사자에게 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 JCA 및 계약에 명시된 의무만큼 개인정보를 보호하는 조항이 포함된 서면 계약을 체결하지 않은 상태에서 개인정보를 제3자에게 공개하거나 이전하지 않는다.
   4. 계약에 명시되거나 본 JCA에 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 관행을 충족 또는 초과하며 개인 데이터 침해로부터 개인정보를 합리적으로 보호할 수 있는 조치로써 본 JCA의 요구 사항을 충족하기에 충분한 방식으로 개인정보 처리를 담당하는 모든 직원에 대한 교육 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. 개인정보 침해가 실제로 발생하였거나 발생하였음이 합리적으로 의심되는 경우, 이를 발견한 당사자는 부당한 지체 없이 상대방 당사자에게 이를 고지(모든 경우에 개인 데이터 침해를 인지한 후 24시간 이내)하고 적절한 조치를 결정하기 위해 상대방 당사자와 협력한다.
   8. 다음 사건 발생 시 모든 경우에 24시간 이내로 부당한 지체 없이 상대방 당사자에게 신속하게 고지한다.
      1. 계약과 관련된 개인정보와 연관이 있는 관할 데이터 보호 또는 기타 규제 당국의 불만 사항, 문의, 요청 또는 우려 사항
      2. 개인정보 액세스, 정정, 수정, 교정, 공유, 삭제 또는 처리 중단 등 데이터 보호법이나 각 당사자의 개인정보 보호 정책에 따른 모든 권리 행사 요청을 비롯하여 계약과 관련이 있는 개인정보와 연관된 데이터 주체의 불만, 문의, 요청 또는 우려 사항
   9. 상대방 당사자가 요청한 조치로서 당사자들이 데이터 보호법 및 본 JCA에 따라 각자의 의무를 준수하는 데 필요한 합리적이고 적절한 모든 조치를 수행한다.
   10. 적용 가능한 법률에서 달리 요구하는 경우를 제외하고 공동 목적을 달성하는 데 필요한 기간 이상 개인정보를 보관하지 않는다.
   11. 본 JCA의 적용을 받는 개인정보의 정확성과 무결성을 유지한다.
   12. 계약과 관련하여 개인정보가 수집 되는 모든 데이터 주체에게 계약의 조건에 따라 고지하고 동의를 얻는다.
   13. 개인정보가 해당 고지, 동의, 허가 및 권리에 따라서만 처리되었으며 본 JCA에서 허용되는 바에 따라 그리고 각 당사자가 데이터 보호법을 준수하는 방식으로 개인정보가 처리되었음을 입증하는 데 필요한 모든 기록을 유지한다.
   14. 어느 당사자가 개인정보의 국경 간 이전을 제한하는 국가 또는 지역의 데이터 주체에 관한 개인정보를 처리하는 경우, 당사자들은 데이터 보호법을 준수하여 처리해야 하며 이는 표준 계약 조항 또는 이와 유사한 개인정보 이전 보호 메커니즘의 체결 등을 포함할 수 있다.
   15. 더 높은 수준의 산업 표준 또는 데이터 보호법을 준수하기 위해 변경 사항을 적용하는 경우를 제외하고 양 당사자는 상대방 당사자가 계약과 연관된 프라이버시 및 데이터 보안 관행에 대해 가장 최근에 수행한 모든 실사와 관련하여 상대방 당사자에게 공개한 각자의 프라이버시 및 데이터 보안 관행을 실제적으로 유지하고 이를 일관되게 적용해야 한다.
   16. 각 당사자는 본 JCA를 체결함으로써 JCA에 명시된 제한 사항의 이해 및 준수를 확인한다는 사실을 인정하고 이에 동의한다.
4. *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, 사용 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 데이터 보호법을 준수하는 방식으로 해석된다.
5. 해석.
   1. “포함하다” 및 “포함”이라는 단어는 제한 없이 포함한다는 의미로 해석된다.
   2. 본 계약에 따른 공동 목적과 관련하여 당사자들은 하나 이상의 상대방 당사자 계열사의 개인정보를 처리할 수 있다. 그러한 경우, 해당 계열사가 계약 또는 본 JCA의 당사자로 지정되었는지 여부와 관계없이 해당 계열사는 개인정보의 “컨트롤러”이자 본 JCA의 제3자 수혜자로 간주되며 본 JCA에 따라 부여된 모든 권리와 보호에 의존하고 이를 집행할 자격이 있다.
   3. 본 JCA는 계약에 통합되어 계약의 일부를 구성한다.
   4. 계약 조항과 본 JCA 조항 사이에 충돌이 발생하는 경우 본 JCA의 조항이 우선한다. 단, 계약 조항이 계약과 관련하여 처리되는 개인정보를 더 높은 수준으로 보호하는 경우에는 보호 수준이 더 높은 해당 계약 조항이 우선한다.
   5. 본 JCA의 조항과 표준 계약 조항 사이에 충돌이 발생하는 경우 표준 계약 조항의 규정이 우선한다.
   6. 여기에 명시적으로 개정된 경우를 제외하고 계약 조항은 완전한 효력을 유지한다.
   7. 본 JCA가 영어와 외국어로 작성되고 영어 텍스트와 외국어 텍스트 사이에 차이가 있는 경우 영어 텍스트가 우선한다.
   8. 본 JCA의 장 및 기타 제목은 참조의 편의를 위한 것일 뿐이며 본 JCA의 의미나 해석의 일부를 구성하거나 이에 영향을 미치지 않는다.
   9. 본 JCA의 첨부 자료 및 부록은 본 JCA 내에 명시적으로 규정된 것과 같은 수준으로 본 JCA의 일부를 구성하는 것으로 간주된다.
   10. 본 JCA의 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 JCA의 나머지 부분은 완전한 효력을 유지한다.
   11. 본 JCA는 동일한 여러 개의 사본이 허용되며 각 사본은 모두 함께 하나의 동일한 계약을 구성한다. 어떠한 당사자든 이러한 사본에 서명∙날인함으로써 본 JCA를 체결할 수 있다.
   12. 본 JCA는 본 JCA의 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 JCA의 어떠한 내용이나 당사자의 어느 일방도 허위 진술에 대한 책임을 배제하려고 시도하지 않는다.
   13. 계약의 준거법과 관할권 규정은 본 JCA에 적용된다.
6. *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 “Joint Controller Addendum” 하의 가장 최근 문서가 다음 발동 이벤트까지 이 JCA의 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 JCA의 조건에 즉각적인 수정이 필요한 상황이 있을 수 있으며, 이는 오직 6(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.com](mailto:privacy_updates@msd.com)에서 통지를 받기를 요청한 모든 단체에 새로운 조항을 통보한 후 30일 이내에 이의가 제기되지 않는 한 그러합니다.  
      1. 적용 가능한 데이터 보호 법률이 기존 JCA의 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.
7. *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.
8. *고지.* 본 JCA에 따라 제공되는 고지(각 “고지”)는 서면으로 이루어져야 한다. 본 JCA에 따라 제공되는 고지는 적용 가능한 계약의 고지 규정에 부합하는 방식으로 이루어져야 하며 이와 함께 이메일을 통해 사본을 [msd\_privacy\_office@msd.com](mailto:msd_privacy_office@msd.com)으로 발송하되 제목란에 “공급업체의 JCA 고지” 또는 개인 데이터 침해의 경우 “긴급: 개인 데이터 침해 고지”를 입력한다.

**부록 1 – 정보 기술 보안 조치**

1. **네트워크 보안** - 공급업체는 네트워크 보안 정책, 절차 및 시스템을 유지 관리해야 하며 공급업체 업계의 모범 사례와 일치하는 네트워크 보안 및 활동을 수행해야 한다. 이러한 활동은 최소한 네트워크 방화벽 프로비저닝, 침입 탐지 및 정기(어떠한 경우에도 연 1회보다 잦은 빈도) 취약성 평가를 포함하되 이에 국한되지 않는다. 어떠한 경우에도 회사의 개인정보에 적용되는 상기 내용은 공급업체가 동일하거나 유사한 성격의 자체 데이터 및 시스템을 보호하기 위해 적용하는 내용보다 덜 엄격하거나 보호 수준이 낮아서는 안 된다.
2. **애플리케이션 보안** - 공급업체는 알려진 비슷한 산업 관행 또는 아래 제9항에 명시된 기준을 이용하여 계약에 따른 서비스 또는 제품과 관련하여 제공 또는 사용되는 모든 소프트웨어 및 시스템과 후속 업데이트, 업그레이드 및 버그 수정을 제공, 유지하며 취약성으로부터 보안을 유지해야 한다.
3. **데이터 보안** -계약 또는 본 JCA에 따른 개인정보를 포함한 기밀 유지 의무 또는 회사 또는 그 계열사의 데이터 및 기타 정보를 보호해야 하는 기타 의무를 제한함 없이, 공급업체는 모든 개인정보를 업계 모범 사례를 따르고 적용 가능한 모든 법률을 준수하여 저장해야 하며 암호화 및 방화벽을 포함하되 이에 국한되지 않는 보안 조치를 사용하여 해당 개인정보가 무단 공개 또는 사용되지 않도록 보호해야 한다. 이러한 조치는 공급업체가 유사한 성격의 자체 데이터에 대해 유지하는 조치보다 엄격해야 한다. 공급업체가 개인정보를 제3자의 오프사이트 시설에 저장하는 경우 공급업체는 제3자에게 개인정보를 공개하거나 서비스 또는 제품을 제3자에게 하도급하는 것과 관련하여 본 JCA의 조항을 준수해야 하며 회사가 합리적으로 허용할 수 있는 제3자의 오프사이트 저장 시설만 사용해야 한다. 이러한 제3자 시설은 전술한 내용을 제한하지 않으며 본 부록의 모든 조항을 완전히 준수하여야 한다.
4. **데이터 저장** - 모든 개인정보는 지정된 공급업체 컴퓨팅 및 저장 리소스에서만 저장, 처리 및 유지되며, 어떠한 개인정보도 어떠한 때이든지 휴대용, 노트북 컴퓨팅 장치 또는 휴대용 저장 매체에서 처리되거나 위 장치 또는 매체로 이전되지 않는다. 단, 해당 장치나 저장 매체가 공급업체가 지정한 백업 및 복구 프로세스의 일부로 사용 중이고 아래 제6항에 따라 암호화된 경우는 예외로 한다. 공급업체는 지정된 백업 및 복구 프로세스의 일부로 모든 백업 개인정보를 저장해야 한다.
5. **데이터 전송** - 회사 및/또는 제3자와의 모든 개인정보 전자 전송 또는 교환은 안전한 수단(HTTPS 또는 SFTP 또는 이에 상응하는 수단 사용)을 통해 아래 제6항에 따라 이루어져야 한다.
6. **데이터 암호화** - 공급업체는 모든 회사 백업 데이터를 포함하여 휴대용, 노트북 컴퓨팅 장치 또는 휴대용 저장 매체에 저장된 모든 개인정보를 상업적으로 지원되는 암호화 솔루션을 사용하여 암호화된 형식으로 보관해야 한다는 데 동의한다. 암호화 솔루션은 대칭 암호화의 경우 128비트 키 이상, 비대칭 암호화의 경우 2048 (또는 그 이상) 비트 키 길이로 배포된다.
7. **데이터 재사용** –본 계약에 따라 서비스나 제품을 제공하기 위하여 필요한 경우나 본 JCA에 따라 달리 허용되는 경우를 제외하고 공급업체는 개인정보를 공급업체의 다른 애플리케이션, 환경 또는 사업부 전반에 걸쳐 배포, 용도 변경 또는 공유할 수 없다.
8. **보안 침해 고지 -** 개인 데이터 침해 또는 공급업체의 보안 의무 위반이 발생한 경우, 공급업체는 계약 또는 JCA에 따른 의무를 이행하는 것 외에 발견 후 24시간 이내로 다음 전화번호 및 이메일을 통해 해당 사건을 회사에 알려야 한다.

보안 침해 고지 전화번호: 704-345-6700

Merck Global Operations Center(“GOC”)(“IT 서비스 차질” 옵션을 선택한다 (이 옵션은 현재 1번이다. GOC는 Merck 사이버 개인 데이터 침해 대응 팀에 연락할 수 있다.)

보안 침해 고지 이메일: [GOC@Merck.com](mailto:GOC@Merck.com)

1. **산업 표준** – 계약에 따른 서비스 또는 제품에 적용 가능한 경우, 일반적으로 인정되는 업계 표준은 다음에 의해 명시 및 유지되는 현재 표준 및 벤치마크를 포함하나 이에 국한되지 않는다.
   1. 인터넷 보안 센터 - <http://www.cisecurity.org> 참조
   2. 결제 카드 산업/데이터 보안 표준(PCI/DSS) - <http://www.pcisecuritystandards.org/> 참조
   3. 미국 국립표준기술연구소 - <http://csrc.nist.gov> 참조
   4. 연방 정보 보안 관리법(FISMA) - <http://csrc.nist.gov> 참조
   5. ISO/IEC 27000 시리즈 - <http://www.iso27001security.com/> 참조
   6. 구조화된 정보 표준 발전을 위한 조직(OASIS) - <http://www.oasis-open.org/> 참조
   7. 오픈 웹 애플리케이션 보안 프로젝트(OWASP)의 “상위 10대 프로젝트” – <http://www.owasp.org> 참조
   8. 공통 취약성 목록(CWE) – <http://cwe.mitre.org> 또는 CWE/SANS 상위 25개 프로그래밍 오류 - <http://cwe.mitre.org/top25/> 참조
   9. SANS 연구소- <http://www.sans.org> 참조
   10. 가장 위험한 소프트웨어 오류 <http://www.sans.org/top25-programming-errors/>

**부록 2**

회사 또는 공급업체가 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 첨부자료 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 JCA의 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 JCA에 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 JCA에 따라 요구되는 모든 고지 및 계약에 따라 요구되는 유사한 고지는 공급업체가 본 JCA를 위반하거나 위반하려고 시도하는 경우에도 필요하다.
      2. 본 JCA의 조항과 관련하여 동의를 수집해야 하는 경우 공급업체는 계약 종료 후 3년 동안 모든 동의의 증거 또한 보관해야 한다.