최종 갱신일: 2021년 6월 22일

데이터 처리 부록

본 데이터 처리 부록(이하 **'DPA'**)은 Lincoln Electric Company 최종 사용자 라이선스 계약서(이하 **'EULA'**)의 부록이며 EULA에 따른 Lincoln Electric Company(이하 **'데이터 처리자/데이터 프로세서'**)와 허가된 사용자(이하 **'데이터 관리자/데이터 컨트롤러'**) (각자 **'당사자'**로 칭하며 함께는 **'당사자들'**로 칭함) 간에 적용되는 내용이다.

그 내용은 다음과 같다.

EULA는 허가된 사용자가 라이선스 애플리케이션을 사용할 수 있는 권리와 해당하는 경우 Lincoln Electric Company에서 제공하는 기타 온라인 서비스를 사용할 수 있는 권리를 규율한다. EULA에 따른 계약 의무 이행 목적상 데이터 처리자 역할은 허가된 사용자 대신 Lincoln Electric Company가 맡는다. 당사자들은 개인 데이터 관련 규정 준수를 보장할 수 있도록 EULA에 데이터 처리자가 데이터 관리자 대신 처리하는 개인 데이터에 적용되는 이용 약관을 정의하는 보충 내용을 추가하는 것에 동의한다.

따라서 다음과 같은 내용에 동의한다.

1. 정의

1.1 본 DPA에 대문자로 표시된 용어[주: 영문 버전에서 대문자로 표시된 것을 뜻함]는 EULA가 다르게 정의하거나 맥락에 따라 달리 정의해야 하지 않는 한 다음과 같은 의미로 해석하도록 한다.

'데이터 관리자(데이터 컨트롤러)'	개인 데이터 처리 목적과 방법을 판단하는 단체를 뜻한다.
'데이터 처리자(데이터 프로세서)'	데이터 관리자 대신 개인 데이터를 처리하는 단체를 뜻한다.
'정보 주체'	식별되었거나 식별이 가능한 인물로 개인 데이터가 처리되는 대상을 뜻한다.
'지침'	데이터 관리자가 EULA에 따른 서비스 제공을 위한 개인 데이터 처리를 위해 데이터 처리자에게 제공하는 지침을 뜻한다.
'개인 데이터'	식별되었거나 식별이 가능한 인물과 관련된 모든 정보를 뜻한다. 이때 식별이 가능한 인물이란 특히 이름, 신분증 번호, 위치 데이터, 또는 온라인 식별자를 통해, 아니면 해당 인물의 물리적, 생리적, 유전적, 정신적, 경제적, 문화적, 또는 사회적 신원에 구체적으로 적용되는 하나 또는 그 이상의 요소를 통해 직・간접적으로 식별이 가능한 사람을 뜻한다.
'개인 데이터 유출'	전송되거나, 저장되거나, 기타 방식으로 처리된 개인 데이터의 불법적인 파괴, 손실, 수정, 무단 공개, 또는 이에 대한 접근을 야기하는 보안 침해를 뜻한다.
'처리'/'처리하는'/'처리된'	수집, 기록, 정리, 저장, 개조나 수정, 획득, 참고, 사용, 송신/보급/전송/기타 방법을 통한 공개, 정렬이나 조합, 제한, 삭제나 파괴 등 개인 데이터에 수행된 모든 행위를 뜻한다.
'처리 서비스'	데이터 처리자가 EULA와 관련해 개인 데이터를 처리하는 것을 뜻한다.
'개인 데이터의 특별 범주'	인종이나 출신 관련 정보, 정치적 의견, 종교적이거나 철학적인 신념, 노조/협회/단체 소속 여부, 외모, 범죄 기록 및 보안 조치, 재정 및 부동산 관련 정보, 거처 관련 정보 또는 신용 정보, 그리고 유전적 데이터, 자연인의 독특한 신원을 드러내는 것이 목적인 개인 데이터, 자연인의 성생활이나 성적 지향과 관련된 데이터, 또는 14세 이하 미성년자와 관련된 데이터의 처리를 뜻한다.
'표준 계약 조항'	제3의 국가에 설립된 데이터 처리자에게 개인 데이터를 전송하는 문제에 관한 표준 계약 조항 관련 EU 집행 위원회 판결 2010/87(2010년 2월 5일 채택)이나 당사자들이 동의한 기타 대체 표준 계약 조항을 뜻한다. 데이터 관리자가 유럽

연합 밖의 관할권에 설립된 단체인 경우, 표준 계약 조항 내 약관의 대부분에 등장하는 “회원국”이라는 단어는 데이터 관리자가 설립된 관할권을 말하는 것으로 이해하면 된다.

‘하청 업체(보조 데이터 처리자)' 데이터 처리자가(아니면 데이터 처리자의 또 다른 하청 업체가) 서면 하청 계약의 지침과 조건에 따라 데이터 관리자 대신 개인 데이터를 처리하는 데 사용하는 모든 처리자를 뜻한다.

1.2 설명과 섹션 표제는 참고와 편의 목적으로만 사용해야 하며, 본 DPA의 일부가 아니고, 본 DPA를 해석하는 방법으로 사용될 수 없다.

2. 본 DPA의 범위와 적용

2.1 본 DPA는 데이터 처리자가 EULA에 따라 데이터 관리자에게 제공하는 처리 서비스와 관련된 EULA 내 약관을 보충하는 용도로만 사용된다.

3. 데이터 처리

3.1 데이터 처리자는 본 DPA에 정의된 약관에 따라 개인 데이터를 처리할 것임에 동의하며, 특히 다음과 같은 내용을 약속한다.

3.1.1 데이터 관리자를 대신하여, 항상 본 DPA에 정의된 데이터 관리자 지침과 모든 해당 데이터 보호 관련법에 따라 개인 데이터만을 처리한다.

3.1.2 처리 서비스를 맡긴 직원 모두가 기밀 유지 조항 준수를 약속한 상태이거나 법적으로 적절한 기밀 유지 의무가 적용되는 상태임을 보장한다.

3.1.3 본 DPA의 스케줄 2에서 설명된 것과 같이 개인 데이터의 보안과 기밀성을 보장하고 데이터 관리자 대신 처리한 개인 데이터의 남용과 손실을 적절하게 방지하기 위한 기술적, 물리적 및 조직적 조치를 취한다.

3.1.4 다음이 발생하는 경우 이를 데이터 관리자에게 즉시 알린다. (a) 형법 집행 기관이나 정보 수사의 기밀성을 유지할 수 있도록 형법에 따라 외부 알림이 금지되는 경우처럼 이를 알리는 것이 금지되는 경우를 제외하고, 정부 단체가 법적으로 구속력이 있는 개인 데이터 요청을 진행하는 경우, (b) 데이터 관리자 대신 처리한 개인 데이터에 영향을 주는 개인 데이터 유출이 발생하는 경우, (c) 데이터 주체가 직접 요청을 전달하는 경우(접근권, 수정권, 삭제권, 이의 제기권, 제한권, 데이터 전송권, 그리고 프로파일링을 포함하여 전적으로 자동화된 결정의 대상이 되지 않을 권리 포함). 데이터 처리자는 이때 (i) 데이터 주체에게 본인이 데이터 관리자 대신 작업을 하고 있음을 알리고 데이터 주체에게 데이터 관리자의 연락처를 주는 것 외에는 그 요청에 직접 응답하지 않는다. 그리고 (ii) 처리의 성격을 고려해 데이터 관리자가 데이터 주체의 권리 행사 요청에 응답해야 하는 의무를 완전히 이행할 수 있도록 적절한 기술적, 물리적 및 조직적 조치를 통해 최대한 데이터 관리자를 돕는다.

3.1.5 통상적으로 합리적인 방식을 통해 데이터 관리자가 개인 데이터 보안 관련 법적 의무를 준수할 수 있도록 협력한다. 이는 적절한 규제 기관에 개인 데이터 유출을 알리는 것, 영향을 받은 데이터 주체에 해당 개인 데이터 유출을 알리는 것, 그리고 해당하는 경우 처리의 성격과 데이터 처리자가 사용할 수 있는 정보를 고려해 데이터 보호 영향 평가를 시행하고 규제 기관과 사전 협의를 하는 것 등이 해당할 수 있다.

3.1.6 데이터 관리자가 본 DPA에 설명된 의무를 준수하고 있음을 증명하는 데 필요한 모든 정보를 제공하고, 감사 진행을 허용하며 이에 기여한다. 이는 섹션 6에 정의된 것과 같이 데이터 관리자가 수행하거나, 데이터 관리자의 필수 요건에 따라 기타 감사관이 수행하는 검사를 포함한다.

3.1.7 하청 업체(보조 데이터 처리자)가 수행하는 처리 서비스가 섹션 7의 내용에 따라 수행되도록 한다.

3.2 데이터 관리자는 준거법의 개인 데이터 처리 관련 내용에 따라 처리 서비스에 적용되는 모든 요건 준수와 데이터 처리자에게 발행되는 지침을 모두 책임진다. 데이터 관리자는 특히 (i) 개인 데이터의 정확함, 품질, 그리고 적법성, (ii) 데이터 주체에서 필요한 동의와 허가를 모두 획득하는 것 등을 포함하여 개인 데이터 수집과 사용에 필요한 모든 투명성 및 적법성 관련 요건을 준수하는 것, (iii) 데이터 관리자가 데이터 처리자에게 개인 데이터를 전송하거나 이를 제공할 권리가 있으며, 데이터 관리자가 해당 전송이나 접근, 그리고 더 일반적으로 본 EULA(본 DPA 포함)의 조건에 따른 데이터 처리에 관련된 필수 동의 및/또는 허가를 모두 제공하였음을 보장하는 것, 그리고 (iv) 그 지침이 준거법을 준수한다는 것을 보장하는 것이 전적으로 본인의 책임임을(앞서 말한 일반적인 내용을 침해하지 않는 방식으로) 인정하고 이에 동의한다. 데이터 관리자는 데이터 처리자의 요청에 따라 데이터 처리자에게 영업일 기준 3일 이내에 해당 통지, 동의 및 허가에 대한 서면 증거를 제공하도록 한다. 데이터 관리자는 본인이 서면으로 별도의 특별 동의를 제공하지 않은 한, 처리 서비스에 개인 데이터의 특별 범주 관련 내용을 입력하거나 기타 방식으로 이를 데이터 처리자에게 제공하지 않는다. 데이터 관리자는 본인이 본 DPA에 정의된 의무를 준수할 수 없는 경우 데이터 처리자에게 즉시, 그리고 불필요한 지연 없이 이를 알리도록 한다. 제공되는 보안 설명서 및 기능을 포함하여 처리 서비스가 본인의 요건, 사업 요건, 그리고 법적 의무를 충족하는지를 확인하는 것은 전적으로 허가된 사용자의 책임이다.

3.3 데이터 관리자는 데이터 처리자가 본 EULA에 따라 처리하는 개인 데이터를 익명화해 라이선스가 부여된 애플리케이션 및 Lincoln 제품과 장비 사용에 관련된 통계 데이터를 얻을 수 있도록 허가한다. 데이터 처리자가 이렇게 얻은 통계 데이터를 계속 사용하더라도 여기에 데이터 관리자의 사전 허가가 필요하지는 않다.

4. 국제 데이터 전송

4.1 데이터 관리자는 데이터 처리자가 EULA에 따른 처리 서비스를 제공하기 위해 처리 서비스 제공 목적으로 미국이나 데이터 처리자가 소재한 기타 국가 내의 개인 데이터를 이동하거나 보관할 수 있음을 인정하고 이에 동의한다. 따라서 처리 서비스 제공 과정에서 데이터 관리자가 설립된 국가 밖에 소재한 데이터 처리자에게 개인 데이터를 전송해야 할 수도 있다. 데이터 관리자가 유럽 경제 지역이나 스위스에 소재한 경우, 당사자들은 데이터 관리자(표준 계약 조항에 따라 데이터 수출자 역할을 하는)가 데이터 처리자(표준 계약 조항에 따라 데이터 수입자 역할을 하는)에게 개인 데이터를 전송하는 작업에 표준 계약 조항의 약관을 적용할 것임을 약속한다.

4.2 당사자들은 데이터 관리자가 유럽 경제 지역이나 스위스 밖에 소재한 경우에도 역시 데이터 관리자(표준 계약 조항에 따라 데이터 수출자 역할을 하는)가 데이터 처리자(표준 계약 조항에 따라 데이터 수입자 역할을 하는)에게 개인 데이터를 전송하는 작업에 표준 계약 조항의 약관을 적용할 것임을 약속한다. 이때 표준 계약 조항은 데이터 관리자가 EULA에 따라 데이터 처리자에게 개인 데이터를 전송하는 작업에 필요한 데이터 보호 규정의 요건 준수가 법적으로 필요하며 그 요건을 충족할 수 있어야 한다.

4.3 당사자들이 본 DPA 섹션 4.1 또는 4.2에 따른 표준 계약 조항을 적용하는 경우...

4.3.1 표준 계약 조항 별첨 1의 내용은 다음과 같이 적용하도록 한다. (a) 데이터 수출자: 데이터 관리자, (b) 데이터 수입자: 데이터 처리자, (c) 데이터 주체: 데이터 관리자(허가된 사용자)의 직원, (d) 데이터 범주: 본 EULA에 따라 라이선스가 부여된 애플리케이션이 모니터링하는 데이터로, 데이터 처리자가 소유하였거나, 라이선스를 제공했거나, 관리하는 제품 및 장비의 사용과 관련되었으며, 등록 데이터(예: 사용자 이름 및 비밀번호 등)를 포함하는 것, (e) 개인 데이터의 특별 범주: 해당 없음, 그리고 (f) 처리 작업: 수집, 복사, 전송/이동, 저장, 수정, 삭제 및 기타 EULA에 따른 처리 서비스에 필요한 작업.

4.3.2 표준 계약 조항 별첨 2의 목적상 데이터 수입자 역할을 하는 데이터 처리자가 취하는 기술적, 물리적 및 조직적 조치의 설명은 본 DPA 스케줄 2에 설명된 내용을 따르도록 한다.

4.4 당사자들에게 섹션 4.1 또는 4.2에 따른 표준 계약 조항이 적용되는 경우, 그 약관은 당사자들이 표준 계약 조항을 섹션 4.5에 따른 독립된 문서로 실행하지 않는 한 참조에 의해 본 약관으로 통합된 것으로 간주된다.

4.5 당사자들은 해당 데이터 보호 규정의 요건에 따라 표준 계약 조항을 별도 문서로 작성하고 실행하도록 한다.

5. 종료

5.1 본 DPA는 EULA의 발효일에 효력을 발휘한다.

5.2 본 DPA는 (a) EULA 또는 (b) 데이터 처리자의 처리 서비스 관련 의무 종료 또는 만료 중 더 늦게 발생하는 사건과 함께 자동 종료되며, 이는 법원 명령, 법원 절차, 또는 데이터 처리자/데이터 관리자/기타 제삼자의 조치 없이도 효력을 발휘한다. 해당되는 경우, 본 DPA가 종료되면 데이터 처리자는 본인이 보유하였거나 관리하는 데이터 관리자의 개인 데이터를 모두 데이터 관리자에게 돌려주거나 데이터 관리자의 요청에 따라 삭제하도록 한다. 데이터 처리자는 데이터 관리자의 요청에 따라 해당 의무 준수를 서면으로 확인하고, 준거법에 따라 개인 데이터를 필수로 보관해야 하거나 준거법이 기타 방식으로 개인 데이터 유지를 허용하는 경우를 제외하고 존재하는 사본을 모두 삭제하도록 한다.

5.3 데이터 관리자는 데이터 처리자가 본 DPA의 내용에 대한 중대한 위반이나 지속적인 위반을 행하였고 그것이 (구제책을 행사할 수 있는 위반이라면) 데이터 처리자가 데이터 관리자로부터 위반 내용을 알리고 구제책을 요청하는 통지를 받은 날로부터 영업일 기준 30일 이내에 교정/배상되지 않은 경우, 데이터 처리자에게 서면으로 종료를 통지하고 본 DPA를 종료할 수 있는 자격이 있다.

5.4 데이터 처리자는 데이터 관리자가 본 DPA의 내용에 대한 중대한 위반이나 지속적인 위반을 행하였고 그것이 (구제책을 행사할 수 있는 위반이라면) 데이터 관리자가 데이터 처리자로부터 위반 내용을 알리고 구제책을 요청하는 통지를 받은 날로부터 영업일 기준 30일 이내에 교정/배상되지 않은 경우, 데이터 관리자에게 서면으로 종료를 통지하고 본 DPA를 종료할 수 있는 자격이 있다.

6. 감사 및 정보 요청

6.1. 데이터 관리자는 정상 업무 시간 중에 데이터 처리자의 영업 활동을 불합리하게 방해하지 않는 방식으로 직접 데이터 처리자에 대한 감사를 실시하거나 기밀 유지 의무가 있는 제삼의 감사자를 임명해 해당 감사를 실시할 수 있다. 이때 감사는 1년에 한 번으로 제한되며 데이터 관리자는 이를 30일 전에 미리 통지해야 한다(단, 규제 기관이 요청하는 감사의 경우는 제외).

6.2. 본 섹션 6에 따라 감사가 발생하는 경우 데이터 처리자는 이에 협력하며 데이터 관리자가 해당 감사를 실시하는 데 필요한 모든 정보를 제공하도록 한다. 본 섹션 6에 따라 발생하는 감사와 관련해 각 당사자에게 발생하는 모든 금액과 비용은 데이터 관리자가 충당하도록 한다.

7. 하청 업체(보조 데이터 처리자)의 임명

7.1 데이터 관리자는 데이터 처리자가 EULA 관련 서비스 이행을 위해서만 [https://www.lincolnelectric.com/en/Legal-Information/Subprocessors]의 링크로 확인할 수 있는 페이지에 나열된 하청 업체의 서비스를 사용할 수 있도록 허가한다.

7.2 데이터 관리자는 데이터 처리자가 하청 업체 변경 15일 전에 데이터 관리자에게 이를 통보하는 경우 새로운 하청 업체의 서비스를 사용할 수 있게 허가한다. 데이터 관리자는 본인에게 알려진 하청 업체의 변경에 동의하지 않는 경우 통지 기간 내에 서면으로 본 DPA를 종료할 수 있다. 데이터 관리자가 통지 기간 내에 본 DPA를 종료하지 않는다면 이는 데이터 관리자의 통지된 하청 업체 변경에 대한 공식적인 동의로 간주된다.

7.3 어떠한 경우라도 데이터 처리자가 하청 업체의 서비스를 사용하게 되면, 하청 업체는 계약을 통해 본 DPA에 따라 개인 데이터 처리와 관련하여 데이터 처리자에게 적용되는 동일한 의무를 준수해야 한다.

8. 기타 약관

8.1 본 DPA의 개정 또는 내용 추가는 서면으로 작성되어야만 유효하다. 앞서 말한 내용에도 불구하고 데이터 처리자는 해당 개정이 개인 데이터의 보안, 기밀성, 또는 무결성에 실질적인 영향을 주지 않는 한 데이터 관리자에게 통지를 하지 않고 언제든지 스케줄 2에 정의된 기술적, 물리적 및 조직적 조치를 개정할 수 있다.

8.2. 본 DPA에서 “서면” 또는 “서면으로”라는 것은 이메일 소통과 내용 증명 우편을 포함한다.

8.3 본 DPA의 특정 약관이 무효화되어도 나머지 조건의 유효성에는 영향이 가지 않는다. 본 DPA의 특정 약관이 무효화되는 경우, 당사자들은 무효화된 약관을 초기 약관과 최대한 동일하거나 동등한 법적 구속력이 있는, 시행 가능하고 유효하며 합법적인 다른 약관으로 대체할 수 있도록 선의의 노력을 해야 한다.

8.4 본 DPA는 EULA와 같은 준거법을 적용 받는다.

스케줄 1 - 특정 관할권에 적용되는 조건

데이터 관리자가 본 스케줄 1에 나열된 관할권 중 하나에 설립된 단체라면 DPA에는 다음과 같은 조건이 적용되며, 본 DPA의 기타 약관과 충돌이 발생할 경우 다음과 같은 해당 조건이 그 내용을 대체하도록 한다. EULA 내 조건 중 본 스케줄에 포함된 적용 관할권의 구체적인 조건에 따라 구체적으로 수정되지 않은 내용은 모두 변경 없이 완전한 효력을 유지한다.

브라질:
당사자들은 DPA의 내용에 다음과 같은 변경 사항이 적용됨을 인정하고 이에 동의한다.

a) DPA에 "개인 데이터의 특별 범주"라는 용어가 언급된 부분은 모두 "민감한 개인 데이터"로 대체한다.

멕시코:
당사자들은 DPA 내용에 다음과 같은 변경 사항이 적용됨을 인정하고 이에 동의한다.

a) DPA에 "개인 데이터의 특별 범주"라는 용어가 언급된 부분은 모두 "민감한 개인 데이터"로 대체한다.
b) 표준 계약 조항의 적용 목적상 개인 데이터의 "전송"이라는 말이 언급된 부분은 모두 멕시코 연방 개인 정보 보호법의 민간 업체가 보유한 개인 데이터 보호 관련 내용에 따른 개인 데이터 이동(*'Ley Federal de Protección de Datos Personales en Posesión de los Particulares'*)의 의미로 해석하도록 한다.

러시아:
당사자들은 DPA의 약관과 함께 다음과 같은 내용을 약속한다.

a) 데이터 처리자는 이로써 본인이 DPA에 따른 개인 데이터 처리 활동의 목적이 처리 서비스 제공뿐임을 완전히 인지하고 있으며, 개인 데이터가 공개된 목적과 데이터 관리자가 데이터 처리자에게 요구한 목적으로만 개인 데이터를 처리하도록 해야 함을 확인한다. 데이터 처리자는 또 데이터 처리자의 요청에 따라 이 규칙을 준수하고 있음을 서면으로 즉시 확인해야 한다.
b) 데이터 관리자는 러시아 국적자의 개인 데이터를 데이터 처리자에게 공개하기 전에 이러한 개인 데이터가 방식에 상관없이(인터넷을 통한 수집 포함) 수집 당시 모두 러시아 연방의 영토에 소재한 데이터를 사용해 기록되고, 체계화되고, 축적되고, 저장되고, 수정되고(갱신, 변경), 추출되었음을 보장해야 한다.
c) 데이터 관리자는 개인 데이터의 불법 처리나 부정확함을 발견한 경우 즉시 데이터 처리자에게 이 개인 데이터를 차단할 것을 지시하고 조사를 진행하도록 한다. 영향을 받은 개인 데이터는 조사 기간 내내 차단된 상태를 유지한다. 해당 조사가 개인 데이터의 부정확함을 확인하는 경우, 데이터 관리자는 관련 데이터 주체나 데이터 보호 기관(해당 경우)에 개정을 요청하고 이를 데이터 처리자에게 전달한다. 부정확한 개인 데이터는 속히 개정하도록 하며, 늦어도 데이터 처리자에게 개정 내용이 전달된 날로부터 7일 이내에는 개정되어야 한다. 해당 개인 데이터는 개정 후 즉시 차단을 해제하도록 한다.
d) 데이터 관리자는 개인 데이터의 불법 처리를 발견한 경우, 즉시 데이터 처리자에게 발견 일자로부터 영업일 기준 3일 이내에 개인 데이터의 불법 처리를 중단할 것을 지시한다. 위반 사항을 제거하고 개인 데이터 처리의 적법성을 보장하는 것이 불가능해 보인다면 데이터 관리자는 데이터 처리자에게 발견 일자로부터 영업일 기준 10일 내에 불법으로 처리된 개인 데이터를 파기할 것을 지시한다. 데이터 관리자는 또 위반 사항 제거를 관련 데이터 주체(또는 그 대리인)에게 알릴 의무가 있으며, 법이 요구하는 경우에는 데이터 보호 기관(해당 경우)에도 이를 알려야 한다.
e) 데이터 주체가 개인 데이터 처리에 대한 본인의 동의를 철회하는 경우, 데이터 관리자는 즉시 이를 데이터 처리자에게 알리고, 데이터 처리자는 취소 통지를 받은 일자로부터 30일 이내에 이 데이터 주체의 개인 데이터 처리를 중단하고 해당 데이터를 파기하도록 한다.
f) 이 문서의 위 조항 d)와 e)에 정의된 기간을 준수하는 것이 불가능한 경우, 데이터 처리자는 데이터 관리자의 요청에 따라 관련 개인 데이터를 최대 6개월간 차단하고, 준거법에 따라 다른 규정이 있지 않은 한 같은 기간 내에 이 개인 데이터를 파기하도록 한다.

남아프리카:
당사자들은 아래 설명된 DPA 섹션 1의 정의에 다음과 같은 변경 사항이 적용됨을 인정하고 이에 동의한다.

a) "정보 주체"란 개인 데이터가 처리되는 사람을 말한다.
b) "개인 데이터"란 식별되었거나 식별이 가능한 인물과 관련된 모든 정보를 포함하는, POPIA에 정의된 것과 같은 개인 정보를 뜻한다.

c) “POPIA”란 2013년 남아프리카 개인 정보 보호법(Act 4), 그리고 POPIA에 따라 발표되어 법적인 구속력을 발휘하는 모든 규정, 지시, 판결, 명령, 또는 지침을 뜻한다.

<u>미국</u>:

당사자들은 DPA의 약관과 함께 다음과 같은 내용을 약속한다.

a) 각 당사자는 처리 서비스에 전송된 개인 데이터의 수집과 공개가 (i) 개인 데이터의 판매가 아니며, 당사자 중 어느 쪽도 이를 개인 데이터의 판매로 간주할 의도가 없고, (ii) 허가된 사용자가 데이터 처리자에게 금전적이나 비금전적인 대가를 지불하는 경우, 해당 금전적/비금전적 대가는 개인 데이터 공개가 아니라 처리 서비스 사용을 위해 제공되는 비용임을 인정하고 이에 동의한다. 데이터 처리자는 처리 서비스 수행이라는 구체적인 목적 외의 다른 목적으로, 또는 법이나 EULA가 허용하지 않는 기타 방식으로 개인 데이터를 유지하거나, 사용하거나, 공개하거나, 판매할 수 없다. 의심의 여지를 없애기 위해, 데이터 처리자는 법이나 EULA가 허용하지 않는 기타 방식으로 개인 데이터를 판매하거나, 하청 업체의 개인 데이터 판매를 허가하거나, 기타 방식으로 이를 허용할 수 없음을 명시한다.

스케줄 2 - 데이터 처리자가 취하는 보안 조치

1. 사업장 및 시설의 물리적 접근 통제

데이터 처리자는 사업장과 시설에 대한 접근을 막기 위해, 그리고 특히 무단 접근 방지를 보장하기 위한 권한 확인 목적으로 기술적 및 조직적 조치를 취한다.

이는 특히 다음을 포함할 수 있다.

- 접근 통제 시스템
- 신분증 판독기, 자기(자석) 카드, 칩 카드
- 열쇠 발급
- 문 잠그기
- 보안 직원, 경비
- 감시 시설
- 경보 시스템, 비디오/CCTV 모니터

2. 시스템 접근 통제

데이터 처리자는 IT 시스템의 무단 접근을 방지할 수 있도록 사용자 식별과 인증을 위한 기술적(ID/비밀번호 보안) 및 조직적 조치를 취한다.

이는 특히 다음을 포함할 수 있다.

- 비밀번호 관련 절차 (특수 문자, 최소 길이, 비밀번호 변경 절차 등 포함)
- 자동 차단 (예: 비밀번호나 시간 제한)
- 분리 가능 매체와 이동식 매체를 포함한 데이터 매체 암호화.

3. 논리적 데이터 접근 통제

데이터 처리자는 할당된 권한이 적용되지 않는 IT 시스템의 활동을 방지할 수 있도록 필수 요건 정의 인증 방식을 활용하고 접근을 모니터링하며 기록한다.

이는 특히 다음을 포함할 수 있다.

- 역할 기반 접근 권한 (프로필, 역할, 거래 및 대상)
- 유지 보수나 기타 관리 목적으로 상용 접근 허용 계정 관리 솔루션을 활용해 사업 계정의 보안 인증을 용이하게 함
- 자동화된 보고서를 정기적으로 검토하고 이례적이거나 의심이 가는 활동에 대한 후속 조치를 실행함
- 최소 권한 모델을 사용하는 접근 통제를 활용해 필지 상황에 따라서만 시스템 및/또는 데이터 접근을 허용함

4. 공개 및 데이터 보호 통제

데이터 처리자는 데이터 매체(수동 또는 전자)의 데이터 이동, 전송, 소통, 또는 저장에 대한 조치를 채택하고 그 후에 전자 데이터 전송, 데이터 이동 및 전달 통제를 확인하는 방법으로 개인 데이터 공개를 통제한다.

이는 특히 다음을 포함할 수 있다.

- 암호화/터널링
- 전자 서명
- 보안 사건과 알림을 기록하고 지속적으로 모니터링함
- 이동되는 데이터를 암호화하는 전송 보안
- 미사용 데이터의 암호화
- 암호화 키의 정기적인 교대
- 암호화 키에 접근할 수 있는 사람의 제한
- 복잡한 비밀번호를 사용하고 원격 접근 세션마다 2단계 인증 활성화

5. 입력 통제

데이터 처리자는 데이터 작업 후 데이터를 입력한 부분, 변경한 부분, 제거(삭제)한 부분, 그리고 이를 진행한 사람 등을 확인할 수 있는 조치를 포함한 완전한 데이터 관리 및 유지 보수 기록을 보관한다.

이는 특히 다음을 포함할 수 있다.

- 기록 및 보고 시스템

6. 직업 통제

데이터 처리자는 데이터 관리자의 지침에 따라 개인 데이터를 처리하고, 데이터 관리자 및 데이터 처리자 사이의 책임을 분리하는 조치(기술적/조직적)를 취할 것임에 동의한다. 이는 특히 다음을 포함할 수 있다.

- 계약서에 모호하지 않은 단어를 사용함
- 공식적인 커미션 진행 (요청 양식)
- 데이터 처리자 선택 기준
- 계약 이행 모니터링

7. 이용 가능성 통제

데이터 처리자는 데이터의 물리적 및 논리적 보안을 보장하는 조치를 취해 데이터가 실수로, 또는 고의로 파괴되거나 손실되지 않게 이를 확실히 보호한다.

이는 특히 다음을 포함할 수 있다.

- 백업 절차
- 하드 디스크 미러링 예: RAID 기술
- 무정전 전원 장치(UPS)
- 제2의 데이터 센터에 복제되는 원격 또는 디스크 저장 공간(스토리지)
- 정기적으로 갱신되는 안티바이러스(바이러스 검사) 및/또는 맬웨어 방지 소프트웨어, 그리고 기본 거부 기능이 설정되어 있어 애플리케이션을 체크하고 영업 관련 목적의 트래픽만을 허용하는 방화벽 시스템
- 업무 지속성 및 재난 복구 계획

8. 분리 통제

데이터 처리자는 서로 다른 목적으로 수집된 데이터의 분리된 처리를 위한 구체적인 조치를 취해 서로 다른 목적으로 수집된 데이터가 기타 고객 데이터와 섞이지 않고 확실히 분리된 상태로 처리(저장, 개정, 삭제, 전송)될 수 있도록 노력한다.

이는 특히 다음을 포함할 수 있다.

- '내부 클라이언트' 개념 / 사용 제한
- 기능 분리 (제조/테스트)