데이터 처리 계약

https://scratcher.io/ko/data-processing-agreement

표준 버전, 최종 업데이트: 2026년 10월 22일. 본 개인정보 처리계약(Data Processing Agreement)은 귀하가 Scratcher를 사용할 때 귀하와 Scratcher ApS(CVR 38552864, Fruebjergvej 3, 2100 Copenhagen Ø, Denmark) 간 체결되는 계약의 일부를 구성합니다. 본 계약은 GDPR 제28조의 요건을 충족하도록 작성되었습니다.

개인정보 처리계약(Data Processing Agreement)

본 개인정보 처리계약은 고객과 Scratcher 간 계약의 불가분의 일부입니다. 본 개인정보 처리계약이 계약에 첨부된 경우, 이용약관 제10조는 적용되지 않으며 본 개인정보 처리계약이 적용됩니다.

1. 정의

1.1. 문맥상 달리 명시적으로 요구하지 않는 한, 본 개인정보 처리계약에서 사용하는 대문자로 시작하는 용어의 정의는 다음과 같습니다.

- “개인정보 유출(Data Breach)”이란 처리되는 개인정보의 우발적이거나 불법적인 파기, 손실, 변조, 무단 공개 또는 접근을 유발하는 우발적이거나 불법적인 개인정보 보안 침해를 의미합니다.
- “개인정보 관리자(Data Controller)”란 GDPR에 정의된 바와 같이 개인정보 처리의 목적과 수단을 결정하는 고객을 의미합니다.
- “개인정보 처리자(Data Processor)”란 개인정보 관리자를 대행하여 개인정보 처리를 수행하는 Scratcher를 의미합니다.
- “개인정보(Personal Data)”란 본 계약에 따라 개인정보 처리자가 개인정보 관리자를 대행하여 처리하는 식별되거나 식별 가능한 자연인에 관한 모든 정보(GDPR 제4조 제1호)를 의미합니다.
- “GDPR”이란 개인정보 처리와 관련한 자연인의 보호 및 해당 데이터의 자유로운 이동에 관한 2016년 4월 27일자 유럽 의회 및 이사회 규정(EU) 2016/679 및 지침 95/46/EC의 폐지(일반 데이터 보호 규정)를 의미합니다.
- “하위 처리자(Sub-Processor)”란 개인정보 처리자의 임직원을 제외하고, 개인정보 처리계약에 명시된 범위와 목적에 따라 개인정보 처리자의 지시 및 대행으로 개인정보를 처리하기 위해 개인정보 처리자가 선임한 모든 자를 의미합니다.

1.2. 위에서 정의되지 않은 대문자로 시작하는 용어는 문맥상 달리 명시적으로 요구하지 않는 한 본 계약에서 정의된 것과 동일한 의미를 가집니다.

2. 적용 범위

2.1. 본 개인정보 처리계약에 포함된 약관은 개인정보 관리자의 지시 및 대행으로 개인정보 처리자가 수행하는 개인정보 처리에 적용됩니다.

2.2. 본 개인정보 처리계약에서 개인정보 처리자를 지칭하는 경우, 관련 조항은 개인정보 처리자가 선임한 하위 처리자에게도 동일하게 적용됩니다.

3. 개인정보 관리자의 지시 및 처리 조건

3.1. 개인정보 처리자는 개인정보 처리자가 적용받는 EU 또는 회원국 법률에 의해 요구되는 경우를 제외하고는 개인정보의 제3국 이전에 관한 지시를 포함하여 개인정보 관리자의 문서화된 지시에 따라서만 개인정보를 처리해야 합니다. 그러한 경우, 개인정보 처리자는 법률이 중요한 공익상의 이유로 이러한 통지를 금지하지 않는 한, 처리 전에 해당 법적 요건을 개인정보 관리자에게 통지해야 합니다.

3.2. 개인정보 처리자는 고객(고객의 고객 포함)이 서비스 이용 시 업로드하거나 제출하는 정보주체의 카테고리에 속하는 개인정보를 처리해야 합니다. 개인정보 관리자를 대행하여 처리되는 개인정보의 유형 및 정보주체의 카테고리는 본 개인정보 처리계약의 부속서 A에 기재되어 있습니다.

3.3. 양 당사자는 본 개인정보 처리계약 및 서비스 이용 시 개인정보 관리자가 성립시킬 수 있는 계약을 개인정보 관리자의 문서화된 지시로 간주하는 데 동의합니다. 개인정보 관리자는 서비스 설정을 조정하여 개인정보 수집에 관한 추가적인 문서화된 지시를 개인정보 처리자에게 제공할 수 있습니다. 양 당사자는 또한 개인정보 관리자의 추가 지시 이행 및 그 비용에 대해 서면으로 합의할 수 있습니다.

3.4. 개인정보 처리자는 서비스 이용 시 개인정보 관리자가 업로드하거나 전송한 시점부터 해당 정보가 삭제될 때까지 개인정보를 처리하되, 본 개인정보 처리계약 제12조에 명시된 기간을 초과하지 않습니다.

3.5. 개인정보 처리자는 지시 사항이 GDPR 또는 기타 EU/회원국의 데이터 보호 규정을 위반한다고 판단되는 경우 즉시 개인정보 관리자에게 통지해야 합니다.

3.6. 개인정보 관리자는 개인정보 처리자의 요청이 있는 경우, 개인정보 처리자가 개인정보 관리자를 대행하여 개인정보를 처리할 때 GDPR의 모든 요건을 적절히 준수하는 데 필요한 정보, 문서 또는 지원을 지체 없이 제공할 것을 약속합니다.

4. 개인정보의 비밀유지

4.1. 개인정보 처리자는 서비스를 제공하고 본 계약에 따른 권리를 행사하는 목적에만 개인정보를 사용해야 합니다. 법률에서 달리 요구하지 않는 한, 개인정보 처리자는 개인정보를 제3자에게 공개해서는 안 됩니다.

4.2. 개인정보 처리자는 업무 수행이나 개인정보 처리자에 대한 서비스 제공을 위해 데이터가 필요한 개인정보 처리자의 임직원 또는 공급업체에게만 개인정보 접근 권한이 부여되도록 해야 하며, 개인정보 처리를 승인받은 모든 사람이 비밀유지를 서약했거나 적절한 법적 비밀유지 의무를 지고 있는지 확인해야 합니다.

4.3. 개인정보 처리자가 법률 요건 준수를 위해 개인정보를 제3자(예: 수사기관)에게 공개해야 하는 경우, 법률에서 달리 금지하지 않는 한 개인정보 처리자는 즉시 개인정보 공개 요건을 개인정보 관리자에게 통지해야 합니다.

4.4. 이러한 비밀유지 의무는 본 개인정보 처리계약이 종료된 후에도 유효합니다.

5. 기술적·조직적 조치

5.1. 기술 수준, 이행 비용, 처리의 성격·범위·맥락 및 목적, 그리고 자연인의 권리와 자유에 대한 위험의 가능성과 심각성을 고려하여, 개인정보 처리자는 개인정보 처리 전 및 처리 기간 내내 개인정보의 안전성을 확보하는 데 필요한 적절한 기술적·조직적 조치를 이행해야 합니다. 적정한 보안 수준을 확보하기 위한 기술적·조직적 조치를 선정하고 이행함에 있어, 개인정보 처리자는 특히 정보주체의 개인정보

처리, 그리고 전송·저장 또는 달리 처리된 데이터의 우발적이거나 불법적인 파기, 손실, 변조, 무단 공개 또는 불법적 접근으로 인해 발생하는 위험을 고려해야 합니다.

5.2. 개인정보 처리자는 해당 분야의 전문가로서 서비스 제공에 관한 지식과 경험을 보유하고 있으므로, 본 개인정보 처리계약 제5.1조에 명시된 목적을 달성하는 데 필요한 기술적·조직적 조치를 선정하고 결정해야 하며, 이러한 조치는 어떠한 경우에도 관련 법률의 요건을 준수해야 합니다. 그럼에도 불구하고 개인정보 관리자는 기술적·조직적 보안 조치 적용과 관련하여 개인정보 처리자에게 지시 및 제안을 할 권리를 가집니다. 개인정보 처리자는 개인정보 관리자의 이러한 제안을 고려하여 검토한 후, (i) 개인정보 관리자의 지시를 이행할 방법에 대한 사유를 담은 답변을 개인정보 관리자에게 제공하거나, (ii) 해당 조치를 이행하기 위한 즉각적인 조치를 취해야 합니다.

5.3. 본 개인정보 처리계약 체결 시점에 개인정보 처리자가 이행한 기술적·조직적 조치는 부속서 C에 기술되어 있습니다. 개인정보 처리자는 ISO/IEC 27001 인증을 받은 정보보안 경영시스템을 유지하며, 전체적인 보안 수준이 저하되지 않는 한 시간이 지남에 따라 조치를 업데이트할 수 있습니다.

5.4. 개인정보 처리자는 처리의 성격과 보유한 정보를 고려하여 GDPR 제32조에 따른 의무를 준수할 수 있도록 개인정보 관리자를 지원해야 합니다.

6. 개인정보 처리 감사

6.1. 개인정보 처리자는 유효한 ISO/IEC 27001 증명서 및 요청 시 적용성 선언서(Statement of Applicability)를 포함하여, GDPR 제28조에 규정된 의무 준수를 입증하는 데 필요한 모든 정보를 개인정보 관리자에게 제공해야 합니다.

6.2. 개인정보 처리자가 개인정보를 적절히 처리하고 있는지 확인하기 위해, 개인정보 관리자는 다음 조건하에 해당 처리에 대한 점검을 실시할 권리를 가집니다. (i) 감사는 개인정보 처리 내용에만 국한되어야 함, (ii) 개인정보 관리자는 최소 4주 이상의 합리적인 기간 전에 감사 실시 의사를 개인정보 처리자에게 통지해야 함, (iii) 감사는 개인정보 처리자의 일상 업무를 방해하지 않는 방식으로 수행되어야 함, (iv) 감사는 개인정보 관리자의 비용으로 수행되어야 함, (v) 감사는 개인정보 처리자가 사전 승인한 독립된 자에 의해 수행되어야 하며(승인은 정당한 이유 없이 거부될 수 없음), 해당 자는 개인정보 처리자의 비밀정보를 보호할 것을 약속해야 함.

6.3. 개인정보 처리자는 감사 수행 지원에 대한 대가를 받을 권리가 있습니다. 해당 대가 금액은 감사와 관련하여 개인정보 처리자에게 발생한 비용을 고려하여 개인정보 처리자가 결정합니다. 개인정보 처리자는 감사 전에 대가 금액을 개인정보 관리자에게 통지해야 합니다.

6.4. 관할 감독기관이 실시하는 감사 및 점검에는 제6.2조 및 제6.3조의 조건이 적용되지 않습니다.

6.5. 개인정보 관리자가 감사 결과에 만족하지 않는 경우, 개인정보 관리자는 재판 외 절차를 통해 본 개인정보 처리계약 및 계약을 일방적으로 해지할 권리를 가집니다. 이 경우 계약 해지는 개인정보 관리자가 취할 수 있는 유일한 조치이며, 개인정보 처리자는 개인정보 관리자의 손해를 배상할 의무가 없습니다.

7. 하위 처리자

7.1. 개인정보 관리자는 이에 따라 본 개인정보 처리계약에 명시된 범위와 목적 내에서 개인정보 처리자를 대행하여 개인정보를 처리할 하위 처리자를 선임하는 것에 대한 일반적인 사전 동의를 개인정보 처리자에게 부여합니다.

7.2. 개인정보 처리자는 선임된 하위 처리자와 서면 계약을 체결했는지 확인해야 하며, 해당 계약에 따라 하위 처리자는 본 개인정보 처리계약에 규정된 것과 동일한 데이터 보호 의무를 준수할 것을 약속해야 합니다. 특히 처리가 GDPR 요건을 충족하도록 적절한 기술적·조직적 조치를 이행할 수 있는 충분한 보증을 제공해야 합니다. 개인정보 처리자는 하위 처리자의 의무 이행에 대해 개인정보 관리자에게 책임을 집니다.

7.3. 현재 하위 처리자 목록은 본 개인정보 처리계약의 부속서 B에 명시되어 있습니다. 개인정보 처리자는 예정된 변경 발생 최소 14 calendar일 전에 개인정보 관리자가 확인할 수 있도록 정보를 제공함으로써 하위 처리자의 교체 또는 신규 선임 계획을 개인정보 관리자에게 통지해야 합니다.

7.4. 개인정보 처리자가 본 개인정보 처리계약 제7.3조에 규정된 절차에 따라 통지한 후 하위 처리자의 교체 또는 신규 선임 이후에도 개인정보 관리자가 서비스를 계속 사용하는 경우, 개인정보 관리자가 개인정보 처리자의 이러한 조치에 동의한 것으로 간주됩니다. 개인정보 관리자가 하위 처리자의 교체 또는 선임에 동의하지 않는 경우, 개인정보 관리자는 재판 외 절차를 통해 계약을 일방적으로 해지할 권리가 있습니다. 이 경우 계약 해지는 개인정보 관리자가 취할 수 있는 유일한 조치이며, 개인정보 처리자는 개인정보 관리자에게 어떠한 손해도 배상할 의무가 없습니다.

7.5. 개인정보 관리자가 하위 처리자 선임에 대한 일반적 동의를 철회하는 경우, 개인정보 처리자는 재판 외 절차를 통해 계약을 일방적으로 해지할 권리를 가지며, 이러한 해지는 중요한 사유로 이루어진 것으로 간주되고, 개인정보 관리자는 해당 해지로 인해 어떠한 손해도 입지 않은 것으로 간주됩니다.

8. 개인정보 유출

8.1. 개인정보 처리자는 개인정보에 영향을 미치는 개인정보 유출이 발생한 경우, 영업 제안서(Sales Proposal)에 명시된 이메일 주소 또는 지정된 주소가 없는 경우 개인정보 관리자의 계정 소유자 이메일 주소로 부당한 지연 없이, 늦어도 개인정보 유출을 인지한 후 24시간 이내에 개인정보 관리자에게 통지해야 합니다. 또한 제공되는 서비스의 성격, 개인정보 처리 및 이용 가능한 정보를 고려하여 다음 정보를 개인정보 관리자에게 제공해야 합니다. (i) 가능한 경우 정보주체의 카테고리 및 대략적인 인원을 포함한 개인정보 유출의 성격, (ii) 개인정보 유출로 인한 발생 가능한 결과, (iii) 발생 가능한 부정적 결과를 완화하기 위한 조치를 포함하여 개인정보 유출에 대응하기 위해 개인정보 처리자가 이행했거나 취할 것을 제안하는 조치, (iv) 추가 정보를 제공할 수 있는 개인정보 보호책임자 또는 기타 담당자의 성명 및 연락처 정보.

8.2. 개인정보 처리자는 개인정보 유출과 관련된 사실, 그 영향 및 취해진 시정 조치를 포함하여 모든 개인정보 유출 사항을 문서화해야 합니다. GDPR 또는 기타 관련 법령에서 규정한 경우, 개인정보 처리자는 해당 문서를 감독기관에 제공해야 합니다.

8.3. 처리의 성격과 이용 가능한 정보를 고려하여, 개인정보 처리자는 GDPR 제33조 및 제34조에 따른 의무를 준수할 수 있도록 개인정보 관리자를 지원해야 합니다. 감독기관 및 필요한 경우 정보주체에게 통지할 책임은 개인정보 관리자에게 있습니다. 본 개인정보 처리계약에 따른 개인정보 처리자의 의무 위반으로 인해 개인정보 유출이 발생한 경우를 제외하고, 제8.1조의 통지를 넘어선 개인정보

처리자의 지원에는 추가 비용이 부과될 수 있습니다.

9. 제3국으로의 개인정보 이전

9.1. 개인정보 처리자가 수행하는 제3국(EU/EEA 역외)으로의 모든 개인정보 이전은 개인정보 관리자의 문서화된 지시에 따라서만 이루어져야 하며, 항상 GDPR 제V장의 규정을 준수해야 합니다.

9.2. 부속서 B에 명시된 하위 처리자에 대한 개인정보 관리자의 승인은 해당 하위 처리자가 수행하는 기술된 데이터 이전에 대한 문서화된 지시를 구성합니다. 이러한 모든 이전은 유럽연합 집행위원회의 적정성 결정(인증된 수령인을 위한 EU-US 데이터 프라이버시 프레임워크 포함), 유럽연합 집행위원회의 표준계약조항(SCC) 또는 GDPR 제V장에 따른 기타 이전 도구에 기반해야 합니다.

10. 협력

10.1. 제공되는 서비스의 성격, 고객 데이터 처리 및 이용 가능한 정보를 고려하여, 개인정보 처리자는 GDPR 제32조~제36조에 규정된 의무 [illegible]을 보장하기 위해 개인정보 관리자와 협력해야 합니다. 이를 위해, 그리고 본 개인정보 처리계약에 명시된 범위 내에서만, 개인정보 처리자는 GDPR에 따른 개인정보 관리자의 의무를 적절히 이행하는 데 필요한 요청 정보를 개인정보 관리자에게 제공해야 합니다.

10.2. 특히 신기술을 사용하는 처리 유형이 처리의 성격, 범위, 맥락 및 목적을 고려할 때 자연인의 권리와 자유에 높은 위험을 초래할 가능성이 있는 경우, 개인정보 처리자는 처리 전에 예정된 처리 작업이 개인정보 보호에 미치는 영향 평가를 실시하는 개인정보 관리자를 지원해야 합니다.

10.3. 정보주체, 감독기관 또는 제3자가 법률에 따라 처리되는 개인정보에 관한 정보 제공을 개인정보 처리자에게 요청하는 경우, 개인정보 처리자는 부당한 지연 없이 해당 요청을 개인정보 관리자에게 전달해야 합니다. 개인정보 처리자는 정보주체, 감독기관 또는 제3자의 요청에 대응하고, 개인정보 정정 및 삭제권, 개인정보 이동권, 처리 거부권 및 제한권을 포함되나 이에 국한되지 않는 정보주체의 권리 행사와 관련된 개인정보 관리자의 의무를 이행하는 데 필요한 범위 내에서 개인정보 관리자를 지원할 것을 약속합니다. 개인정보 처리자는 소유한 정보가 법률로 정한 기간 내에 전달되도록 해야 합니다.

11. 개인정보 관리자의 의무

11.1. 개인정보 관리자는 단독 재량과 책임으로 개인정보 처리자에게 제공할 개인정보의 유형과 정보주체 카테고리를 결정해야 하며, 개인정보 처리자의 적절한 서비스 제공에 필요한 개인정보만을 개인정보 처리자에게 제공해야 합니다. 개인정보 관리자는 개인정보 처리자가 필요 이상의 개인정보를 수령하는 위험을 포함하여 수반되는 모든 위험을 부담합니다.

11.2. 개인정보 관리자는 개인정보 처리자에게 개인정보를 제공하고 계약에 따라 개인정보 처리자가 개인정보를 처리하도록 위탁하는 데 필요한 모든 허가 및 권한을 취득하였으며 계약 기간 동안 이를 유지할 것임을 진술하고 보증합니다.

12. 개인정보의 삭제 및 반환

12.1. 계약 또는 본 개인정보 처리계약이 종료되면, EU 또는 회원국 법률에 따라 개인정보 보관이 요구되지 않는 한, 개인정보 처리자는 개인정보 관리자의 선택에 따라 개인정보 관리자를 대행하여 처리된 모든 개인정보를 삭제하거나 개인정보 관리자에게

반환하고(개인정보 관리자는 언제든지 서비스에서 자신의 데이터를 내보낼 수 있음) 기존 사본을 삭제한 후 이를 이행했음을 개인정보 관리자에게 증명해야 합니다. 백업에 저장된 사본은 정상적인 백업 주기 만료에 따라 삭제되며, 그동안 다른 목적으로는 사용되지 않습니다.

13. 책임 규정

13.1. 개인정보 관리자가 입은 손해와 관계없이, 본 개인정보 처리계약에 따른 개인정보 처리자의 전체 책임은 다음과 같이 제한됩니다. 본 개인정보 처리계약에 따라 또는 이와 관련하여 발생하는 모든 청구에 대한 개인정보 처리자 및 그 공급업체의 총 책임은 손해배상 청구 원인 발생일 전 12개월 동안 개인정보 관리자가 서비스에 대해 개인정보 처리자에게 실제 지급한 금액을 초과할 수 없습니다. 관련 법률이 허용하는 최대 범위 내에서, 개인정보 처리자 또는 그 공급업체가 손해 발생 가능성을 사전에 알고 있었거나 구제 수단이 그 본래 목적을 달성하지 못한 경우라 할지라도, 개인정보 처리자 또는 그 공급업체는 특별 손해, 부수적 손해, 간접 손해 또는 결과적 손해(이익, 데이터 또는 기타 정보의 손실, 사업 중단, 인적 상해, 프라이버시 침해로 인한 손해를 포함하되 이에 국한되지 않음)에 대해 어떠한 경우에도 책임을 지지 않습니다.

13.2. 제13.1조의 제한 사항은 양 당사자 간에만 적용됩니다. 관련 법률에 따라 제한될 수 없는 책임에는 적용되지 않으며, GDPR 제82조에 따른 정보주체의 권리에 영향을 미치지 않습니다.

14. 유효 기간 및 해지

14.1. 본 개인정보 처리계약은 계약의 효력 발생과 동시에 효력이 발생하며, 계약이 유효하게 유지되는 한 계속 효력을 가집니다. 개인정보 처리자의 의무는 개인정보 관리자를 대행하여 개인정보를 처리하는 동안 계속됩니다.

15. 최종 조항

15.1. 개인정보 처리자는 개인정보 처리계약의 변경 예정일로부터 최소 30일 전에 변경 사항을 통지해야 합니다. 개인정보 처리계약 변경 공지 후에도 개인정보 관리자가 서비스를 계속 사용하는 경우, 개인정보 관리자가 개인정보 처리계약 변경 사항에 동의한 것으로 간주됩니다. 개인정보 관리자가 변경 사항에 동의하지 않는 경우, 개인정보 관리자는 서비스를 사용할 수 없으며 계약을 해지할 권리가 있습니다.

15.2. 본 개인정보 처리계약과 계약 간에 충돌이 있는 경우, 개인정보 처리에 관해서는 본 개인정보 처리계약이 우선합니다.

15.3. 본 개인정보 처리계약은 계약에 규정된 것과 동일한 법률의 적용을 받으며, 분쟁 역시 동일한 방식으로 해결됩니다.

15.4. 부속서:

- 부속서 A: 개인정보 처리 세부사항;
- 부속서 B: 승인된 하위 처리자;
- 부속서 C: 기술적·조직적 조치

부속서 A – 개인정보 처리 세부사항

주제 및 기간	계약 기간 동안 서비스와 관련하여 수행되는 개인정보 처리 및 제12조에 따라 개인정보가 삭제되거나 반환될 때까지의 이후 처리.
처리의 성격	호스팅 및 저장; 개인정보 관리자의 캠페인 및 양식을 통한 개인정보 수집; 서비스 내 표시, 내보내기 및 삭제; 개인정보 관리자가 설정한 참여자에 대한 이메일 및 메시지 전송(예: 확인, 코드 및 경품 통지); 개인정보 관리자의 지시에 따른 통합, 웹훅(webhook) 및 API를 통한 개인정보 관리자 자체 시스템으로의 이전; 지원 및 오류 처리.
개인정보 처리 목적	개인정보 관리자가 계약에서 합의된 바에 따라 개인정보 처리자의 서비스를 사용할 수 있도록 지원.
개인정보 처리 작업	서비스 이용 중 제공된 개인정보를 포함한 고객 데이터의 수집 및 저장.
개인정보 유형	이름, 성, 이메일, IP 주소 및 이를 통해 도출된 대략적인 위치, 가입 일시(created at), 생일 및 전화번호와 같은 추가 데이터(고객이 수집하는 경우). 개인정보 관리자가 캠페인을 설정하는 방식에 따라 캠페인 질문에 대한 답변, 게임 결과 및 당첨된 경품, 코드, 동의 기록, 참여자가 업로드한 파일(예: 이미지) 및 브라우저·기기 정보와 같은 기술 데이터도 포함됨.
특수 범주의 데이터	대상 아님. 서면으로 합의하지 않는 한 개인정보 관리자는 서비스를 통해 특수 범주의 개인정보(GDPR 제9조) 또는 범죄 처벌에 관한 데이터(GDPR 제10조)를 수집해서는 안 됨.
정보주체 범주	개인정보 관리자(고객) 캠페인의 참여자, 가입하지 않은 개인정보 관리자 캠페인 방문자(IP 주소, 대략적인 위치 및 브라우저 정보), 데이터가 개인정보 관리자를 대행하여 처리되는 범위 내의 개인정보 관리자의 서비스 사용자.
개인정보 처리 장소	개인정보는 개인정보 처리자의 사옥 및 유럽연합 내에 위치한 가상 서버, 그리고 부속서 B에 명시된 하위 처리자의 해당 위치에서 처리됨.
처리 기간/보유 기간	개인정보 관리자가 서비스 내에서 설정한 바에 따름. 이용약관 제9.4조에 따라 개인정보 처리자는 3년이 지난 개인정보를 삭제할 수 있음.

부속서 B – 승인된 하위 처리자

개인정보 처리계약 체결 시점에 개인정보 관리자는 아래에 명시된 하위 처리자의 선임을 승인합니다. EU/EEA 역외로의 이전은 수령인이 인증된 EU-US 데이터 프라이버시 프레임워크 또는 유럽연합 집행위원회의 표준계약조항(제9.2조)에 기반합니다.

하위 처리자	처리 내용	처리 장소
Amazon Web Services EMEA SARL, Luxembourg (AWS)	서비스 호스팅: 서버, 데이터베이스, 파일 저장소, 백업, 캐싱 및 로그	유럽연합(스웨덴 스톡홀름). 콘텐츠는 Amazon CloudFront 네트워크를 통해 전달되며, EU/EEA 역외의 엣지 로케이션에서 트래픽을 처리할 수 있음.
ClickHouse, Inc. (ClickHouse Cloud)	IP 주소 및 브라우저 정보를 포함하여 방문, 참여, 가입과 같은 캠페인 통계 분석 데이터베이스	유럽연합(독일 프랑크푸르트), AWS에서 호스팅됨.
Mailgun Technologies, Inc. (Sinch 계열사)	추적이 활성화된 경우 배송, 열람 및 클릭을 포함하여 확인, 코드, 경품 통지와 같이 개인정보 관리자가 설정한 이메일을 참여자에게 전송	유럽연합(메시지 데이터용 EU 리전); 제한된 계정 정보는 전 세계적으로 처리될 수 있음.
ip-api.com	사기 및 보트를 차단하기 위해 참여자 IP 주소의 대략적인 위치를 조회하고 프록시 및 데이터 센터의 트래픽을 감지	루마니아(EU); EU/EEA 역외에서의 처리 또는 데이터 이전을 배제할 수 없음.
Google (Gemini API)	AI 어시스턴트, 번역, 텍스트 생성과 같은 서비스 내 AI 기능. 개인정보 관리자의 사용자가 직접 입력하지 않는 한, 참여자 데이터는 익명화되거나 집계된 형태(예: 이니셜, 이메일 도메인, 가입 시간)로만 전송됨	미국 및 API 엔드포인트와 처리 구성에 따라 잠재적으로 기타 국가.
Functional Software, Inc. (Sentry)	오류를 찾아 수정하기 위한 서비스의 오류 모니터링 및 세션 리플레이. 보고서에는 내부 사용자 및 계정 ID와 개인정보 관리자 사용자의 브라우저에 대한 기술 데이터가 포함될 수 있음. 세션 리플레이의 텍스트는 마스킹 처리됨	유럽연합(독일, Sentry EU 리전).
Cloudflare, Inc. (Turnstile)	개인정보 관리자가 캠페인에 대해 활성화한 경우에만 캠페인 양식에서 보트 보호 기능 제공. 참여자의 IP 주소 및 브라우저 신호를 수신함	글로벌 네트워크; EU/EEA 역외에서 처리가 발생할 수 있음.

하위 처리자	처리 내용	처리 장소
Features & Labels, Inc. (fal.ai)	서비스 내 AI 이미지 생성 및 편집, 배경 제거 및 음성 더빙. 개인정보 관리자의 사용자가 제출하는 프롬프트와 이미지를 수신함	미국.
Adressevælger (adressevaelger.dk)	개인정보 관리자가 캠페인에 대해 활성화한 경우에만 캠페인 양식에서 주소 추천 기능 제공. 참여자가 입력하는 주소 텍스트와 참여자의 IP 주소를 수신함	덴마크(EU).

부속서 C – 기술적·조직적 조치

개인정보 처리자는 Bureau Veritas로부터 ISO/IEC 27001:2022 인증을 받은 정보보안 경영시스템을 유지합니다(인증 번호: FIHSK27150F). 조치 항목은 다음과 같습니다.

- **호스팅 및 물리적 보안:** 모든 고객 데이터는 유럽연합 내 Amazon Web Services(AWS) 데이터 센터에 저장됩니다. 개인정보 처리자는 자체 서버를 운영하지 않으며, 물리적 및 환경적 보안은 ISO 27001 및 SOC 2 인증을 받은 AWS에서 제공합니다.
- **네트워크 보안:** 서버 및 데이터베이스는 인터넷에서 접근할 수 없는 전용 네트워크(Amazon VPC)에서 실행됩니다. 로드 밸런서와 콘텐츠 전달 네트워크만 웹 애플리케이션 방화벽(AWS WAF) 및 DDoS 보호 기능으로 보호되어 외부에 공개됩니다.
- **암호화:** 모든 트래픽은 TLS(HTTPS)로 암호화됩니다. 데이터베이스, 파일 및 백업은 AES-256으로 저장 시 암호화(at rest)됩니다. 통합에 사용되는 자격 증명은 애플리케이션 수준에서 추가 암호화됩니다. 비밀번호는 bcrypt로 해시 및 솔트 처리됩니다.
- **접근 제어:** 고객 사용자를 위한 역할 기반 접근 제어, 2단계 인증 및 Google 단일 로그인(SSO), 세션 타임아웃, 로그인 시도 횟수 제한. 임직원의 접근 권한은 최소 권한 및 알고 있어야 할 필요성(need-to-know) 원칙을 따르며, 고유 계정 및 가능한 경우 다중 요소 인증을 사용하고 최소 1년에 한 번 검토하며 퇴사 시 즉시 권한이 회수됩니다.
- **격리:** 고객 데이터는 계정별로 논리적으로 격리(다중 테넌트 격리)되며 모든 요청에 대한 권한이 검증됩니다.
- **로깅 및 모니터링:** 인프라 변경 사항은 위변조 방지 감사 트레일에 기록되고, 애플리케이션 로그는 중앙에서 수집되며, 플랫폼은 24시간 모니터링되고, 고객은 활동 로그에서 사용자의 활동을 확인할 수 있습니다.
- **가용성 및 복구력:** 최소 7일 동안 보관되고 운영 환경과 분리되어 저장되는 일일 암호화 백업, 최소 1년에 한 번 실시하는 복구 테스트, 매년 검토 및 연습되는 비즈니스 연속성 및 재해 복구 계획.
- **침해 사고 관리:** 제8조에 따른 개인정보 유출 통지를 포함하여 보안 사고를 보고, 평가, 차단, 분석 및 사후 조치하기 위한 문서화된 프로세스.
- **안전한 개발 및 운영:** 서버는 수동으로 변경되지 않는 SSH 접근이 없는 변경 불가능한 컨테이너(immutable containers)로 실행되며, 변경 사항은 배포 전에 테스트됩니다.

- **인력 보안:** 임직원은 비밀유지 의무를 지며 정보보안 경영시스템의 일환으로 정보보안 인식 교육을 받습니다. 인프라 접근 권한이 있는 파트너는 스스로 ISO 27001 인증을 받았으며 업무에 필요한 접근 권한만 부여받습니다.
- **데이터 최소화 및 삭제 도구:** 개인정보 관리자는 각 캠페인이 수집할 데이터를 결정하며, 참여자 데이터를 내보내거나 삭제하거나 자동 삭제할 수 있습니다.