



Dashlane의 개인정보 보호정책

당사의 '개인정보 보호정책'은 다음과 같습니다. 당사의 소프트웨어를 이용하려면 개인정보 보호정책에 동의해야 합니다. 물론 이 정책을 이해하기 힘들 수 있습니다. 당사는 귀하가 동의하는 내용을 이해하기를 원하므로, 각 섹션은 간략한 "비법률적" 요약으로 시작됩니다. 요약은 개인정보 보호정책의 일부는 아니지만 정책을 이해하는 데 도움을 드리기를 위한 것입니다.

최종 업데이트: 2021년 2월 10일

1. 개요

요약

본 개인정보 보호정책은 당사가 사용자의 개인정보(특정 개인의 신원을 파악하는 데 사용될 수 있는 정보) 및 익명정보(신원을 파악할 수 없는 정보)를 확보하고 이용하는 방법을 기술합니다. 명시된 바와 같이 본 정책의 특정 부분은 일부 사용자(예: EU 또는 캘리포니아주 거주자)에게만 적용됩니다. 당사는 개정된 개인정보 보호정책을 여기에 게시함으로써 언제든지 변경할 수 있습니다. 중대한 변경 사항은 이메일, 인앱 알림 등을 통해 현재 사용자에게 알려 드립니다. 당사의 서비스 제공을 위해서는 특정 개인정보가 요구되지만, 당사는 필요한 정보만 수집하고자 노력합니다. 승인된 사용자가 아닌 아동(예: 가족 요금제를 함께 사용하는 아동)에 관한 모든 개인정보는 요청 시 삭제됩니다.

- a. **일반:** 본 개인정보 보호정책(이하 “정책”)은 Dashlane, Inc. 및 계열사(“Dashlane” 또는 “당사”)가 당사 웹사이트인 www.dashlane.com(Dashlane 블로그, “사이트” 등 서브도메인 포함) 방문자 및 당사의 모바일 및 데스크톱, 웹 애플리케이션(개별적으로 “앱”, 집합적으로도 “앱”으로 지칭함) 사용자에게 관한 정보를 수집, 사용 및 공유하는 방법을 설명합니다. 앱과 사이트는 합쳐서 “서비스”로 지칭합니다. “귀하” 또는 “사용자”는 서비스 사용자 또는 사이트 방문자를 의미합니다. 본 정책에서 정의되지 않았지만 강조 표시된 용어는 당사의 [서비스 약관](#)(“약관”)에서 의미를 찾을 수 있습니다.
- b. **특정 지역 조항:** 본 정책의 일부는 캘리포니아주 소비자 개인정보 보호법(“CCPA”), 유럽연합의 일반 개인정보 보호법(“GDPR”), 브라질의 LGPD 등 특정 지역의 개인정보 보호법의 영향을 받는 사용자에게만 적용됩니다. 이러한 조항은 명확하게 분류되어 있습니다. 이 분류에 해당하지 않는 경우, 본 정책은 Dashlane 서비스의 모든 사용자에게 동등하게 적용됩니다.
- c. **변경:** 당사는 언제든지 본 정책을 변경할 수 있습니다. 당사가 변경할 경우 당사는 업데이트된 정책이 이 페이지에 게시하며, 변경 사항이 중요한 경우에는 이메일 또는 서비스를 통해 기존 사용자에게 알려 드립니다.
- d. **아동:** 본 서비스는 아동을 대상으로 하지 않습니다. 단, 부모 또는 보호자가 서비스 이용을 허락(가족 요금제 또는 이에 상응하는 요금제를 통해)하는 아동은 이용이 가능합니다. 아동(자녀가 거주하는 관할권을 기준으로 하며, 미국인 경우 만 13세 미만)이 당사에 부모의 동의 없이 개인정보를 제공했음을

인지하게 되면, [지원 센터에 알려 주시기 바랍니다](#). 당사는 신속히 해당 정보를 당사 시스템에서 제거할 것입니다.

- e. **개인정보와 익명정보.** 본 정책에서 사용되는 바와 같이 “개인정보”는 이름, 우편 주소, 이메일 주소, IP 주소 또는 전화번호 등 개인을 식별하는 단독 또는 다른 정보와 결합된 모든 정보를 의미합니다. “익명정보”는 개인의 신원 확인을 허용하지 않는 단독 또는 당사 또는 제3자가 이용 가능한 다른 정보와 결합된 데이터를 의미합니다. 당사는 아래 명시한 대로 개인정보와 익명정보를 모두 수집합니다.
- f. **사용자의 개인정보가 필요한 이유.** 당사는 사용자에게 서비스를 제공하기 위해 특정 개인정보가 필요합니다. 사용자는 해당 개인정보를 제공해 줄 것을 요청받게 되며, 앱을 다운로드 및 사용하려면 본 정책 및 약관에 동의해야 합니다. 이 동의는 언제든지 철회할 수 있으며, 사용자의 개인정보 처리에 필요한 법적 기반을 제공합니다. 사용자는 당사가 요청하는 개인정보를 제공할 의무는 없으나, 당사에 해당 개인정보를 제공하지 않는 경우 당사는 서비스를 제공하거나 문의 사항에 답변할 수 없게 됩니다.

2. 특히 중요한 정보(일부 관할권에 해당)

- a. *(유럽, 영국 및 브라질 사용자).*
 - i. **담당자 소개:** GDPR, LGPD 및 개인정보 데이터 관리자에 대한 정보가 필요함이 규정된 기타 법률의 목적상, 개인정보 데이터 관리자는 21 Rue Pierre Picard, 75018 Paris, France에 소재한 Dashlane SAS입니다. 이메일(dpo@dashlane.com)을 통해 당사의 데이터 보호 담당자와 연락할 수 있습니다.
 - ii. **필독 섹션:** “데이터 보안 및 국제 전송”과 “개인 정보에 관한 귀하의 권리”라는 제목의 섹션을 주의깊게 읽어 주십시오.
- b. *(캘리포니아주 및 네바다주 사용자).*
 - i. **개인정보의 판매:** 귀하는 [개인정보 판매 금지](#) 페이지에서 개인정보의 판매를 거부할 수 있습니다. 당사는 개인정보를 금전 또는 다른 대가(예: 무료 서비스와의 교환)를 위해 교환하지 않습니다. 그러나 "판매(sale)"에 대한 CCPA의 광범위한 정의는 전환 데이터가 추천 광고주에게 전송되는 상황(Dashlane으로 이동되는 광고를 클릭하면 당사가 고유한 식별자를 추천 사이트로 보내 추천 사이트가 추천에 대한 크레딧을 받는 경우)도 포함할 수 있습니다. 당사가 전송하는 정보는 개인정보를 포함하지 않지만, 귀하가 해당 링크를 클릭하고 Dashlane을 방문한 사실이 광고 게시자에 의해 귀하의 프로필에 추가될 수 있습니다. 이 모든 작업은 “퍼블리셔 쿠키”(쿠키 정책에 정의된 바와 같이)를 통해 사이트에서 이루어지며, 개인정보 판매를 거부하면 이 쿠키가 비활성화됩니다.

3. DASHLANE이 데이터를 확보하는 방식은?

요약

당사는 귀하(예: 계정을 만들거나 또는 구독료를 결제하는 경우)나 다른 사람(예: 고용주가 Dashlane를 사용하도록 초대할 경우)이 제공한 데이터 또는 앱이나 쿠키 및 제3자를 통하여 자동으로 확보된 데이터를

수집합니다. 당사가 수집하는 개인정보에는 귀하의 이메일(계정 생성에 사용된) 및 특정 청구 정보(구독의 경우)가 포함되지만, 완전한 결제 정보는 당사의 결제 프로세서에만 저장됩니다. **당사에서는 귀하의 마스터 암호를 알 수 없기 때문에, 귀하가 서비스에 저장한 보안 데이터가 무엇인지 알 수 없습니다.** 당사는 쿠키를 포함한 기술을 활용하여 서비스 제공 및 개선을 위해 사용하는 사용 정보를 수집합니다. 자세한 내용은 당사의 [쿠키 정책](#)에서 확인할 수 있습니다.

당사는 다음과 같은 방식으로 정보를 수집합니다.

a. 사용자 제공 정보.

- **등록 데이터:** 앱을 사용하려면 계정을 생성해야 하며, 이를 위해서는 서비스 로그인에 사용할 유효한 이메일 주소를 제공해야 합니다. *Dashlane 무료 계정 생성에 필요한 개인정보는 이메일 주소뿐입니다.* Dashlane은 귀하가 계정을 삭제한 후 칠(7) 일 동안 등록 데이터를 보관합니다. 유료 계정의 경우 사용자는 아래에 명시된 청구 데이터를 제공해야 합니다. B2B 계정의 경우 등록 데이터는 비즈니스 이름, 우편 주소(송장을 이용해 지불하는 경우)와 관리자 연락처 정보를 포함하며, 사용자의 비즈니스 이메일 주소를 포함할 수 있습니다. **등록 데이터는 반드시 최신 상태로 유지해야 합니다.** 당사는 일부 고객 서비스 요청에 응대하기 위해 귀하가 계정 소유자임을 확인해야 합니다. 계정과 연결된 확인된 이메일 주소나 신원 확인에 사용된 전화번호(해당하는 경우에) 대한 액세스가 유실된 경우 계정이 잠길 수 있으며, 당사는 도움을 드리지 못할 수 있습니다.
- **청구 데이터:** 당사는 제3자 서비스 제공사를 이용하여 사이트에서 발생하는 결제를 처리합니다. 당사는 납세 협력 및 사용자 지원을 목적으로 신용카드의 만료일과 마지막 네 자리 숫자를 보관합니다. 당사는 결제 프로세서의 서비스에 대한 결제 방법과 관련하여 이름, 주소, 전화번호에 액세스할 수 있으나, 이러한 정보는 당사의 결제 프로세서만 저장합니다. 당사는 절대 완전한 신용카드 정보를 보유하지 않으며, 귀하가 Google Play Store 또는 Apple App Store(“**앱 스토어**”)를 통해 구독에 대한 비용을 지불하는 경우 어떠한 청구 데이터도 받거나 보관하지 않습니다. 청구 데이터는 귀하의 계정 삭제 후 최대 칠(7) 일까지 저장됩니다.
- **마스터 암호:** 싱글사인온(“**SSO**”)을 사용하여 서비스에 액세스하는 B2B 계정 구성원 외의 사용자는 각자 “**마스터 암호**”를 만들어야 합니다. 마스터 암호는 구성원의 계정에 액세스하고 구성원이 앱에 저장하는 정보(“**보안 데이터**”, 아래에서 정의됨)를 안전하게 보호하는 암호화 키를 생성하는 데 사용됩니다. 마스터 암호가 안전할수록 보안 데이터도 더 안전해집니다. Dashlane의 Zero Knowledge 기술로 인해 Dashlane은 당사 사용자의 마스터 암호 또는 SSO 암호화 키 생성에 사용된 데이터를 알 수 없으며, 이에 따라 보안 데이터에도 액세스할 수 없습니다. 다른 부정한 수단이나 마스터 키는 없으며, 해커가 어떤 방법으로 당사 서버의 모든 보안 데이터를 획득하더라도 각 계정을 별도로 해킹해야 합니다. 사용자가 그렇게 설정하지 않는 한, 앱은 로컬에 마스터 암호를 저장하지 않습니다. 앱에 마스터 암호를 보관하도록 지정한 사용자의 기기가 도난당하거나 손상된 경우, 해당 사용자의 보안 데이터가 유출될 수 있습니다.
- **보안 데이터:** 당사의 앱에서는 사용자가 신용카드 번호와 사이트 또는 애플리케이션 인증 정보와 같은 민감한 정보를 포함하는 디지털 신원 데이터를 관리할 수 있습니다. 이러한 정보와 사용자가

앱에 저장하는 모든 것은 '보안 데이터(Secured Data)'에 해당됩니다. 보안 데이터는 전송 및 보관 시 항상 암호화되며, 승인된 기기의 로컬에서만 암호 해독이 가능합니다. Dashlane은 전송한 바와 같이 암호화 키에 대한 액세스 권한이 없으므로 Dashlane 서버의 보안 데이터에 액세스할 수 없습니다. Dashlane이 귀하의 보안 데이터를 보호하는 방법을 자세히 알아보려면 [보안 백서](#)를 참고하십시오.

- **지원 및 연락:** 귀하는 당사 사이트의 사용자 지원 요청 및 문의와 연계하여 개인정보를 제공할 수도 있습니다. 사용자 지원 기록은 연계된 계정이 삭제된 후 칠(7) 일 동안 유지됩니다.
 - **피드백:** App Store, Trustpilot 등의 사이트에 리뷰를 게시하거나, Productboard 및 기타 연구 또는 연락을 통해 제안하는 등 당사에 피드백을 제공하는 경우, 당사는 피드백과 함께 제공된 개인정보를 사용하여 귀하에게 답변을 드릴 수 있습니다. 당사는 약관에 설명된 대로 제한 없이 피드백을 사용할 수 있습니다.
 - **기타 데이터.** 또한 해당 정보가 수집된 시점에 당사가 공개한 방법으로 다른 유형의 정보를 수집할 수도 있습니다.
- b. *사용자가 타인에 관해 제공하는 데이터:* 서비스에서 귀하는 다른 사용자가 앱을 사용해 볼 수 있도록 초대할 수 있습니다. 이 기능을 귀하가 사용하는 경우(또는 이 기능으로 귀하가 초대된 경우), Dashlane은 향후 조치를 위해 초대받은 사람의 이메일 주소와 이들에게 전송된 메시지를 저장합니다(그리고 해당되는 경우, 추천 보너스 등으로 추천인에게 크레딧을 제공합니다). 당사는 초대받은 사람에게 자신을 Dashlane에 초대한 사람을 알려 주고 자신의 정보를 당사의 시스템에서 삭제하도록 요청할 수 있는 기회를 제공합니다. 추천인 또는 초대 대상자는 [지원 센터](#)에 해당 정보의 삭제를 요청할 수 있습니다.
- c. *기술적으로 수집한 데이터.*
- **기기 및 브라우저 데이터.** 귀하가 서비스에 액세스할 때 당사는 (해당하는 경우) 자동으로 운영체제 이름 및 버전, 기기 식별자, 브라우저 유형, 브라우저 언어 및 IP 주소를 포함한 정보를 기록합니다. 데이터의 일부는 [쿠키 정책](#)에 설명한 대로 쿠키를 사용하여 수집합니다. 이 데이터는 귀하의 계정 보안을 유지하고, 서비스가 정확한 언어로 제시되고 귀하의 기기에 최적화되도록 하며, 고객 지원을 촉진하고, 세무 및 규제 준수 목적을 위해 사용됩니다(예: IP 주소와 관련된 지역을 활용하여 현지 규제 지침 표시). 이 데이터는 귀하의 계정이 삭제된 후 칠(7) 일 동안 보관됩니다.
 - **이용 데이터(Usage Data).** 당사는 로그를 사용하여 서비스 이용에 관한 데이터(“**이용 데이터**”)를 수집합니다. 당사는 등록 데이터(Registration Data)와 연결된 이벤트 데이터(Event Data), 그리고 완전히 익명인 행동 데이터(Behavioral Data), 이 두 가지 이용 데이터를 유지합니다.
 - “**이벤트 데이터**”는 앱의 자체 기능 이용(예: 활성화된 기능, 보안 데이터에 저장된 자격 증명의 수)에 관한 것으로, 사용자에게 관련된 정보와 지원을 제공하고 서비스를 제공, 분석 및 개선하는 데 사용됩니다. 이벤트 데이터는 서비스와 제3자의 상호작용 방식에 관한 정보를 포함하지 않습니다. 이벤트 데이터는 계정이 삭제된 후에도 유지되지만, 완전히 익명화됩니다. 동일한 사용자가 새 계정을 만들더라도 이전 계정의 이벤트 데이터는 새

계정과 연결될 수 없습니다. 익명화된 이벤트 데이터의 유지는 정확한 서비스 이용 이력 기록을 유지하기 위해 필수적입니다.

- **“행동 데이터”**는 사용자가 서비스 외부에서 어떤 행동을 하는지에 관한 정보(예: 로그인 자동 입력이 사용된 사이트, 사용자가 보안 데이터에 자격 증명을 저장한 사이트 또는 앱)입니다. 예를 들어 앱이 자격 증명을 자동으로 입력하려면 사용자가 로그인하는 사이트를 인식해야 하므로, 행동 데이터는 정상적인 서비스 운영에 중요합니다. 단, 개인의 프라이버시 보호를 위해 행동 데이터는 익명으로 보고 및 기록되며 개인과 연결할 수 없습니다. 행동 데이터는 Dashlane의 소유입니다.

일부 Dashlane 직원은 이벤트 데이터에 액세스하여 서비스 이용을 분석하고 사용자 지원과 기술 지원을 제공할 수 있습니다. 본 서비스에서는 이벤트 데이터와 행동 데이터를 모두 활용하여 상황에 맞는 알림(예: 계정 설정 알림)을 발송하고 집계 데이터를 생성합니다.

- **합산 데이터(Aggregated Data):** 당사는 이용 데이터를 합산하여 당사 서비스의 사용에 관한 추가적인 정보를 추출합니다(예: 특정 관할권 내에 있는 사용자의 수, 가장 인기 있는 기능). 이 **“합산 데이터”**는 익명 데이터로 Dashlane의 소유이며, 주로 서비스의 분석과 개선을 돕는 데 사용됩니다.
 - **쿠키:** [쿠키 정책](#)에 명시된 바와 같이, 당사는 귀하 및/또는 귀하의 기기를 인식하고 귀하가 서비스와 상호작용 시 매끄러운 맞춤형 경험을 제공하기 위해 쿠키 및 유사한 기술을 사용합니다.
- d. **제3자로부터 확보한 데이터:** 당사는 당사의 서비스 제공사(예: 결제 프로세서를 통한 계정 검증의 경우), B2B 계정 관리자를 포함한 기타 사용자(예: 서비스 체험 초대를 받는 경우), 소셜 미디어 계정과 같은 전체 공개 출처, 이러한 정보를 당사와 공유하도록 법적으로 허용된 마케팅 파트너와 조사원 등 데이터 제공사로부터 사용자에게 관한 정보를 수신합니다.

4. DASHLANE이 사용자의 개인 정보를 사용하는 방식은?

요약:

당사는 개인정보를 사용하여 귀하의 계정을 확인하고, 서비스를 제공하고, 사용자를 지원하고, 귀하와 소통하며 마케팅 활동을 조정합니다. 당사는 귀하의 개인정보로 자동화된 결정을 내리거나 프로파일링을 수행하지 않습니다.

- a. **일반:** Dashlane은 개인정보를 이용하여 서비스를 제공하고 홍보하며 다음을 포함한 귀하의 요청에 응답합니다.
- 귀하의 계정 수립 및 유지, 보호.
 - 귀하를 사용자로 식별하고 요청하신 서비스 제공
 - 사기 탐지 및 인증 수행.
 - 사용 데이터를 측정하여 서비스 및 당사와 사용자의 상호작용 개선.
 - 결제 알림 또는 지원 및 유지관리 조언을 포함한 행정적 통보 발송. 귀하가 마케팅 통신문 수신을 거부한 경우에도 이러한 통보문은 받게 됩니다.

- 귀하가 서비스에 액세스하는 권한 또는 귀하가 요구하는 인터페이스 및 옵션 제공.
 - 서비스 내 특정 기능 사용 여부, 사이트의 페이지 방문 여부 또는 당사의 광고 조회 여부를 파악하여 맞춤 정보 제공.
 - 고객 지원 질의 및 기타 요청에 응답.
 - 서비스 홍보 또는 Dashlane의 다른 마케팅 정보 발송(일부 Dashlane 파트너의 제품에 관한 소식 포함). 유럽 및 영국의 사용자를 포함한 일부 사용자는 계정 생성 시 또는 이후 마케팅 통신문 수신에 동의해야 합니다. 기타 지역의 사용자(그리고 유럽 및 영국의 거주자이면서 이전에 수신에 동의한 사용자)는 해당 통신문 수신을 중단하도록 선택할 수 있습니다.
 - 아래에 명시된 대로 제3자 사이트 및 플랫폼의 광고 활동 관리.
- b. *자동화된 의사 결정 및 프로파일링*. 당사는 귀하의 개인정보를 이용하여 자동화된 의사결정을 하지 않습니다.

5. DASHLANE이 개인 정보를 공유하는 방식은?

요약

당사는 절대 사용자의 개인정보를 판매하지 않습니다. 당사는 모든 관련 법률(예: GDPR)을 계약상 준수해야 하며, 관련 서비스 제공에 필요한 데이터에만 액세스할 수 있는 서비스 제공사와 개인정보를 공유합니다. 귀하가 (개인정보를 포함할 수 있는) 보안 데이터를 공유하도록 요구하는 경우, 서비스는 해당 요청을 따릅니다. 당사는 보다 세분화된 광고(예: 활성 사용자가 제3자 사이트와 플랫폼에서 Dashlane 광고를 보지 않도록)를 위해 광고주와 해시 처리 및 암호화된 사용자 이메일과 기기 ID를 공유합니다. 당사는 본 정책의 적용을 받는 계열사 그리고 Dashlane이 매각되거나 합병되는 경우의 인수자와 개인정보를 공유할 수 있습니다. Dashlane B2B 계정 관리자는 해당 요금제의 사용자에게 관한 특정 개인정보와 사용 정보에 액세스할 수 있습니다. 마지막으로, 당사는 법에 의거하여 요구되거나 당사의 권리나 서비스를 보호하는 데 필요하다고 판단되는 경우 개인정보를 공개할 수 있습니다.

Dashlane은 본 정책에 명시되어 있는 경우를 제외하고는 귀하의 개인정보를 판매(일반적인 정의로서의 “판매”를 말하며, 캘리포니아주 관련 내용에서 정의된 “판매”에 대한 정보는 섹션 2(b) 및 8 참조)하거나 사용하지 않습니다. 당사는 귀하의 개인정보를 다음 상황에서 공유합니다.

- 사용자가 지정한 제3자: 서비스는 보안 데이터(개인정보를 포함할 수 있음)를 귀하의 지시대로 제3자와 공유합니다(예: 서비스의 “공유” 기능을 사용할 때). 이러한 데이터가 당사 서버를 통해 전달되는 동안, 당사는 본 정책의 다른 부분에서 언급한 바와 같이 해당 데이터에 접근할 수 없습니다.
- 서비스 제공사: 당사는 계정을 생성하고, 고객 지원을 제공하고, 결제를 처리하거나 귀하와 Dashlane 간 소통에 요구되는 경우 등 서비스를 제공하기 위한 목적으로만 서비스 제공사와 귀하의 개인정보를 공유합니다(예: 고객의 지원 요청에 관련된 개인정보를 zendesk의 당사 대행사에게 제공하는 경우). 당사는 해당되는 서비스 제공사의 보안 및 데이터 프라이버시 관행을 검토하여 해당 법률과 이 정책을 준수하는지 확인합니다. 당사의 데이터 호스팅

제공사(AWS)가 저장하는 보안 데이터는 앞서 기술한 대로 항상 암호화되어 있습니다. 서비스 제공과 관련하여 개인정보에 대한 접근 권한을 가지는 서비스 제공사는 [하위 처리자 명단](#)에 공개되어 있습니다.

- **마케팅:** 당사는 광고를 최적화하기 위해(예: 다른 사이트에서 기존 Dashlane 사용자에게 Dashlane의 광고가 노출되지 않도록 보장) 서비스 제공사에 해시 처리된 이메일 및/또는 기기 ID를 제공합니다. 이러한 제공사가 이와 같은 정보를 일체의 다른 목적(해당 제공사가 유지 및 관리하는 프로필을 늘리기 위한 목적 포함)으로 사용하는 것은 금지됩니다.
- **계열사:** 본 정책은 Dashlane, Inc.가 소유하거나 Dashlane, Inc.의 통제 하에 있는 모든 법인(“계열사”)에 적용됩니다. 당사는 서비스 제공 및 요청에 응답하는 데 필요한 경우 개인정보를 계열사 간에 공유합니다. 일부 계열사는 미국에 위치하고 있는데, 미국은 유럽 규제기관에서 GDPR의 적용을 받는 개인정보를 보관 및 보호하는 데 적합하지 않은 것으로 간주하는 개인정보 보호 및 관련 법이 시행되는 국가입니다. 유럽 법률에서 요구하는 보호 수준을 제공하기 위해 당사는 아래 명시한 수단에 추가하여 EU 및 미국 계열사에 데이터 처리 부록이나 동등한 문서를 구비하고 있습니다. Dashlane의 미국 계열사도 프라이버시 실드 인증을 받았습니다. 자세한 내용은 섹션 10을 참조하십시오.
- **Dashlane B2B 계정 관리자:** Dashlane B2B 계정 관리자는 해당 계정 액세스에 사용된 이메일 주소 및 특정한 이벤트 데이터를 확인할 수 있습니다. 이러한 이벤트 데이터에는 개별 사용자가 저장한 로그인 정보 수(단, 로그인 정보 식별은 불가), 암호 점수, 암호 재사용 여부(단, 암호가 재사용된 사이트나 암호 자체는 확인 불가)가 포함됩니다.
- **기업 구조조정:** 만약 다른 회사가 Dashlane 또는 그 비즈니스나 자산을 인수하거나 합병한 경우, 해당 회사는 그 시점에 당사가 보유한 모든 개인정보를 보유하게 되며, 본 정책에 적시된 당사의 모든 권리와 의무를 승계합니다. 따라서, 당사는 해당 거래와 연계하여 개인정보를 공유할 수도 있습니다. 개인정보 및 기타 정보는 또한 Dashlane의 지급불능 또는 파산, 재산관리 상태가 발생한 경우 사업 자산으로 양도될 수 있습니다.
- **기타 공개:** 당사는 귀하의 개인정보에 대한 기타 공개에 대해 고지하고, 공개 전에 귀하의 동의를 구합니다. 단, 개인정보와 관련하여 귀하의 선택과 상관없이, Dashlane은 (a) 법률 집행 명령, 적용 가능한 법률 또는 정부 명령을 준수하기 위해, (b) Dashlane의 권리, 다른 사용자의 권리 또는 서비스를 보호하는 데 선의로 필요하다고 생각되는 경우, 귀하의 개인정보를 공개할 수 있습니다. 단, Dashlane은 유효한 명령의 대상이 되더라도 당사의 zero-knowledge 기술로 인해 등록 데이터 및 이벤트 데이터 외의 사용자에 대한 정보를 제공할 수 없습니다. Dashlane은 법률에서 허용하는 한 법적으로 요구되는 개인정보를 알려 드립니다.

6. 데이터 보안 및 국제 전송

요약

당사는 다양한 수단을 통해 확보한 개인정보를 포함하여 당사가 보유한 모든 데이터를 보호하기 위해 노력하며, 관련 실무를 지속적으로 개선 및 업데이트합니다. 하지만 당사가 처리하는 개인정보의 보안을

보장할 수 없으며, 보장하지 않습니다. 개인정보는 미국을 포함하여 귀하의 국가에서 적용하는 규정보다 덜 엄격한 개인정보 보호 및 법률을 따르는 관할 법원으로 전송될 수도 있습니다. 하지만 당사는 미국에서 처리 시 유럽과 영국의 규정 및 기타 관련 규정을 준수하는 기술 및 기타 수단을 도입하여 개인정보를 보호하고 있습니다.

- a. 당사는 엄격한 물리적, 체계적, 기술적 및 관리적 수단을 사용하여 당사가 보유하거나 처리하는 모든 데이터를 보호하며, 보안 개선을 위해 당사의 정책과 실무를 정기적으로 재평가하여 수정하고 있습니다. 당사는 귀하의 데이터를 보호하기 위해 최선을 다하지만, 어떠한 데이터 전송 또는 보관 방법도 완벽하게 보안되지는 않으므로 당사는 당사가 관리하는 데이터의 보안을 보장할 수 없습니다. 귀하의 데이터가 당사 또는 서비스 이용으로 인해 침해되었다고 생각하시는 경우, 즉시 [지원 센터](#)로 연락하여 주십시오.
- b. 당사가 귀하로부터 수집한 개인정보를 포함한 귀하의 정보는 당사, 당사의 계열사 및 미국을 포함한 귀하의 본국 이외의 서비스 제공사로 전송, 보관되거나 처리될 수 있습니다. 미국의 데이터 보호 및 개인정보 보호 규정에 따라서는 다른 국가에서와 동일한 수준의 보호가 이루어지지 않을 수도 있습니다. 당사가 데이터의 전송, 보관 및 처리를 실행할 때는 본 정책에 기술된 단계에 따릅니다. 여기에는 당사 또는 당사의 벤더가 처리하는 모든 개인정보를 (생성된 위치와 상관없이) 적용 가능한 법률의 요구에 따라 보호하도록 하는 섹션 5 및 10의 내용도 포함됩니다. 귀하는 서비스를 사용함으로써 본 정책에 의거하여 귀하의 데이터를 전송, 보관 또는 처리하는 것에 동의하게 됩니다.

7. 사용자가 사용자 데이터를 관리하는 방법은?

요약

개인정보의 수정과 개인정보 및 데이터 기본 설정의 조정은 앱의 "계정" 또는 "설정" 섹션에서 할 수 있습니다. 귀하가 현재 마케팅 이메일을 받고 있으나 더 이상 받고 싶지 않다면, 해당 이메일 내에서 수신 거부할 수 있습니다. 이러한 이메일을 수신 거부하더라도 당사는 귀하에게 운영 및 거래와 관련된 이메일을 계속 보냅니다(예: 갱신 통보). 기기에서 앱을 제거하면 그 앱과 관련된 모든 데이터가 제거됩니다. 앱을 제거해도 계정은 삭제되지 않습니다. 이러한 작업을 수행하려면 [여기](#)에서 지침을 참고하십시오.

- a. **정보 및 개인정보 설정 변경**: 앱의 "계정" 또는 "설정" 섹션에 액세스하여 귀하의 계정과 연계된 개인정보와 프라이버시 및 데이터 기본 설정을 수정할 수 있습니다. 도움이 필요한 경우 [지원 센터](#)에 문의하십시오.
- b. **이메일 통신**: 귀하의 동의 하에 당사는 앱 사용 요령과 일부 Dashlane 파트너의 제품 정보를 포함하여 서비스 이용을 홍보하기 위한 이메일을 주기적으로 발송합니다. 각 이메일에 포함된 수신 거부 안내에 따라, 혹은 서비스에서 개인정보 및 데이터 설정을 변경하여 이러한 홍보성 이메일을 수신 거부할 수 있습니다. 또한 [지원 센터](#)를 통해 수신 거부를 요청하실 수도 있습니다. 마케팅 통신문을 수신 거부하더라도, 앱 내에서의 위반 통보 및 기타 알림, 갱신 이메일 등 서비스 운영 및 거래와 관련된 통신문은 거부되지 않습니다.

- c. **애플리케이션.** 앱을 제거함으로써 해당 앱에 의한 정보 수집을 모두 중단시킬 수 있습니다. 해당 기기 또는 플랫폼의 표준 제거 프로세스를 이용할 수 있습니다. 앱을 제거해도 계정은 삭제되지 않습니다. 그렇게 하려면 [여기](#)에서 지침을 참고하십시오.

8. 개인 데이터에 관한 사용자의 권리(EU, 영국, 브라질, 캘리포니아주와 네바다주 사용자)

요약
 EU, 영국, 브라질, 캘리포니아주 및 네바다주의 법률이 적용되는 사용자는 개인정보에 관련된 특정 권리를 보유하고 있습니다. 여기에는 당사와 같은 서비스 제공사가 보유한 개인정보에 액세스하고 이를 수정하며, 서비스 제공사에게 더 이상 관련이 없는 개인정보를 “무시”하도록 할 권리가 포함됩니다. 이러한 권리의 대부분은 서비스의 개인정보 및 데이터 기본 설정에서 액세스되어야 하지만, 언제든지 도움이 필요한 경우 당사에 문의하십시오. 당사는 이러한 권리를 행사하는 어느 누구에게도 결코 질 낮은 서비스를 제공하거나 그런 사람을 어떤 식으로든 처벌하지 않습니다. Dashlane은 해당 법의 의도를 강력하게 지지하며, 귀하가 실질적으로 이러한 권리의 적용을 받지 않더라도 해당 권리에 대한 이행 요청에 부응하도록 최선을 다할 것입니다.

- a. 귀하는 당사가 처리하는 귀하의 개인정보에 대해 다음과 같은 권리를 보유하고 있습니다. 달리 명시된 경우를 제외하고, 이러한 권리는 GDPR(그리고 관련 법률), CCPA 및 LGPD가 해당하는 사용자에게 동등하게 적용됩니다.
 - **동의 철회:** 귀하는 귀하의 개인 정보 전체 또는 일부분(예: 마케팅용)에 대한 처리에 관한 동의를 철회하실 수 있습니다. 일부 서비스는 철회 시 사용하지 못하게 될 수 있습니다.
 - **액세스/정보 요청:** 귀하는 당사가 보유하는 개인 정보에 언제든지 귀하의 계정을 통해 또는 직접 당사에 문의하시어 접근하실 수 있습니다.
 - **수정:** 귀하는 언제든지 당사가 보유한 잘못되거나 오래된 개인정보를 귀하의 계정을 통해 또는 직접 당사에 문의하여 수정할 수 있습니다.
 - **삭제 및 제거.** 당사가 귀하에 관해 보유하는 개인정보가 더 이상 관련이 없거나 정확하지 않은 경우를 포함한 특정 상황에서, 귀하는 귀하의 개인정보를 삭제하도록 당사에 요청할 수 있습니다. 계정을 삭제하면 삭제한 날로부터 일주일 이내에 모든 개인정보가 삭제됩니다.
 - **이동성:** 귀하는 귀하의 개인 정보에 대한 사본을 요청하여 항상 이를 원하는 다른 회사로 이전할 수 있습니다.
 - **개인정보 판매 금지(캘리포니아주 및 네바다주 사용자에게 해당):** 개인정보의 모든 “판매”를 중지하려면 [개인정보 판매 금지](#) 페이지로 이동하십시오. 자세한 방법은 위의 섹션 2(b)를 참고하십시오. 이러한 조치는 관할권에 관계없이 모든 사용자가 취할 수 있습니다.
- b. 이 권리를 행사하려면 앱의 "계정" 또는 "설정" 섹션에서 액세스할 수 있는 "개인정보 및 데이터 설정" 페이지를 통해 요청을 제출하십시오. 도움이 필요하면 [지원 센터](#)에 문의하거나 이메일(support@dashlane.com)을 보내거나 [아래 주소로 문의하십시오.](#) **요청서 작성 시에는 (i) 어떤 개인정보가 대상인지 그리고 (ii) 상기 권리 중 어느 것을 행사하고자 하는지를 명확하게 기재해**

주십시오. 귀하의 보호를 위해, 당사는 귀하가 요청을 보낼 때 이용한 이메일 주소와 연계된 개인정보에 대한 요청만을 이행할 수 있으며, 귀하의 요청을 이행하기 전에 귀하의 신원을 확인해야 할 수도 있습니다. 당사는 귀하의 요청을 즉시 준수하며, 어떠한 경우에도 법적으로 규정된 기한을 넘기지 않습니다(GDPR의 경우 30일, CCPA의 경우 45일). 기록 보존 목적으로 또는 해당 변경 또는 삭제 요청 이전에 귀하가 개시한 거래를 완료하기 위해 특정 정보를 보존할 수도 있습니다.

- c. 당사는 상기 명시된 권리를 행사하는 어떠한 사용자도 차별(예: 불친절한 서비스 제공 또는 더 많은 요금 청구 등)하지 않습니다.

9. 연락처 정보, 불만사항

귀하가 이 정책 또는 당사의 데이터 수집이나 처리 실무에 관해 질문, 우려 또는 불만이 있는 경우, 또는 임의의 보안 위반 사항을 신고하고 싶은 경우, [지원 센터](#), 이메일(support@dashlane.com)로 문의하거나 아래 주소로 서신을 보내주십시오.

Dashlane, Inc.
Attn: Legal
44 West 18th Street., 4th Fl.
New York, NY 10011

스위스, EU 및 영국 사용자 해당 사항: 당사는 신고된 모든 불만 사항을 즉시 해결하고자 하지만, 귀하의 불만이 적절하게 해결되지 않았다고 생각하는 경우에는 언제든지 귀하 거주지의 데이터 보호 감독 당국에 연락할 수 있습니다. 감독 당국의 목록은 [여기](#)를 클릭하여 확인하십시오.

10. 프라이버시 쉴드(PRIVACY SHIELD)

요약

Dashlane 이 EU 및 스위스에 거주하는 시민의 개인정보와 관련하여 특정 보호수단을 제공하는 EU-미국 및 스위스-미국 프라이버시 쉴드 원칙(Privacy Shield Principles)을 준수하고 있다는 점은 미국 상무부에 의해 공식 인증되었습니다. 프라이버시 쉴드는 2020년 7월에 EU에서 무효화되었으나, Dashlane은 당분간 당사의 인증을 유지합니다.

참고: 프라이버시 쉴드(Privacy Shield)는 2020년 7월에 유럽연합에서 무효화되었으나, 당사는 이 원칙을 향한 지속적인 노력을 보여주고 일부에서 예측하는 것처럼 향후 해당 프로그램이 재시작될 때를 대비하여 프라이버시 쉴드 인증을 계속 유지하기로 했습니다. Dashlane은 GDPR의 지속적인 준수를 보장하기 위해 프라이버시 쉴드 대신 GDPR에 따른 유효한 이전 체계를 포함하도록 B2B 고객에 대한 [데이터 처리 부록\(Data Processing Addendum\)](#)을 업데이트했습니다(모델 조항). 더불어 당사 서버는 EU(아일랜드)에 위치하므로, 미국 정부는 서버에 포함된 미국 시민이 아닌 사람의 데이터에 대한 관할권이 없습니다.

- a. Dashlane은 유럽연합과 스위스에서 미국으로 이전되는 개인 정보의 수집 및 사용, 유지에 관해 미국 상무부에 의해 수립된 유럽연합-미국 및 스위스-미국 프라이버시 쉴드 프레임워크를 따릅니다. 당사는 미국 상무부에 당사가 프라이버시 쉴드 원칙을 준수하고 있음을 인증했습니다(상무부의 정의대로). 이 정책과 프라이버시 쉴드 원칙에 상충하는 내용이 있는 경우 프라이버시 쉴드 원칙이 우선합니다.

프라이버시 실드 프로그램과 프라이버시 실드 원칙에 관해 더 자세히 알고 싶거나 당사의 인증을 보고 싶다면 www.privacyshield.gov를 방문해 주십시오.

- b. 프라이버시 실드 원칙 준수에 대한 당사의 인증은 사용자의 개인 정보와 채용과 관련하여 수집된 과거와 현재의 직원 개인 정보 모두에 적용됩니다(“HR 데이터”). Dashlane은 EU 데이터 보호 기관(“DPA”)에 의해 수립된 패널과 협력하고 유럽연합에게서 전달받은 고용관계 맥락 내 HR 데이터와 관련하여 패널로부터 받은 조언을 준수합니다. DPA 연락처 목록은 [여기](#)에 있습니다.
- c. 프라이버시 실드 원칙에 기술된 바와 같이, Dashlane은 Dashlane이 수령하여 추후 제 3자에게 전송하는 개인 정보에 대해 책임을 집니다. 당사를 위해 개인 정보를 처리하는 제 3자가 프라이버시 실드 원칙을 준수하지 않고 개인 정보를 처리하면, 당사는 손상을 야기한 사건에 대한 책임이 없음을 입증하지 않은 그 같은 미준수에 대한 책임을 집니다.
- d. 프라이버시 실드 원칙에 부합하여, Dashlane은 개인 정보 수집 또는 사용에 관한 불만사항을 해결하기 위해 노력합니다. 이 정책에 관한 질의 또는 불만사항이 있는 EU 또는 스위스 거주민은 먼저 지원 센터에 문의하여야 합니다.
- e. Dashlane은 개인정보 보호에 관한 미해결 불만 사항을 미국에 위치한 대안적 분쟁 해결 사업자인 JAMS로 전달합니다. 당사로부터 귀하의 불만사항에 대한 응답을 적시에 받지 못하거나 당사가 귀하의 불만을 해결하지 않은 경우, www.jamsadr.com/eu-us-privacy-shield 페이지를 방문 또는 연락하여 더 자세한 정보를 알아보거나, 불만 내용을 제출하십시오. JAMS 서비스는 무료로 제공됩니다.
- f. 프라이버시 실드 원칙에서 더 자세히 설명했듯이, 다른 방식으로는 해결되지 않는 나머지 불만사항을 다루기 위해 프라이버시 실드 패널 앞에서 선고되는 구속력 있는 중재 역시 이용하실 수 있습니다. Dashlane은 연방무역위원회의 수사 및 집행력의 대상입니다.