Veri İşleme Sözleşmesi (DPA)

Genel Veri Koruma Tüzüğü (GDPR) Madde 28 uyarınca

Version 1.0, son güncelleme: 22 Eylül 2026

Taraflar

Müşteri (GDPR Madde 4(7) anlamında veri sorumlusu):

Firma / Ad: _____

Adres: _____

scryp hesabının e-posta adresi: _____

scryp (GDPR Madde 4(8) anlamında veri işleyen):

Gökhan Sagir, şahıs işletmesi sahibi, scryp markası altında faaliyet göstermektedir
Erdbergstraße 121/9, 1030 Viyana, Avusturya
UID: ATU83108129
Veri koruma iletişim adresi: datenschutz@scryp.at

Bundan böyle “Müşteri” ve “scryp”, birlikte “Taraflar” olarak anılacaktır.

Genel bakış

Müşteri, ses ve video kayıtlarının transkripsiyonunu ve değerlendirmesini yaptırmak için scryp'i kullanır. Bu kayıtlarda, kişisel verilerinden Müşterinin sorumlu olduğu kişiler konuşmaktadır. scryp bu verileri yalnızca Müşteri adına işler. İşbu Sözleşme, scryp'in verilerle ne yapabileceğini, verileri nasıl koruduğunu ve sonunda verilere ne olacağını belirler.

1. Konu ve uygulama alanı

1.1 İşbu Sözleşme, scryp'in Hizmet Koşulları (www.scryp.at/agb adresinden ulaşılabilir) uyarınca scryp hizmetini sunarken Müşteri adına işlediği tüm kişisel veriler için geçerlidir. Hizmetin kullanımına ilişkin sözleşme bundan böyle “Ana Sözleşme” olarak anılacaktır. İşbu Sözleşmenin güncel sürümüne www.scryp.at/avv adresinden ulaşılabilir.

1.2 Sözleşme ilişkisinin kendisine ait veriler, yani Müşterinin hesap, sözleşme, faturalandırma ve destek verileri işbu Sözleşmenin konusu değildir. scryp bu verileri, kendi Gizlilik Politikası (www.scryp.at/datenschutz) uyarınca kendi adına veri sorumlusu olarak işler.

1.3 Ek 1 ila Ek 3, işbu Sözleşmenin ayrılmaz parçasıdır. İşbu Sözleşme ile Ana Sözleşme arasında çelişki olması hâlinde veri koruma konularında işbu Sözleşme önceliklidir.

1.4 İşbu Sözleşme, scryp'i mesleki, ticari veya resmî bir faaliyet kapsamında kullanan müşteriler için öngörülmüştür. Tamamen kişisel kullanımda GDPR, Madde 2(2)(c) uyarınca uygulanmaz ve bir veri işleme sözleşmesi gerekli değildir.

2. İşlemenin niteliği, amacı ve kapsamı

2.1 İşlemenin niteliği ve amacı, veri türleri ve ilgili kişi kategorileri Ek 1'de açıklanmıştır.

2.2 scryp verileri yalnızca Avrupa Birliği üye devletlerinde işler. İşleme yerleri Ek 1 ve Ek 3'te belirtilmiştir.

2.3 İşlemenin süresi, Ana Sözleşmenin süresi ile Madde 12'de düzenlenen silme sürelerinin toplamına karşılık gelir.

3. Talimatlar

3.1 scryp verileri yalnızca Müşterinin belgelenmiş talimatı üzerine işler. Müşterinin talimatları; Ana Sözleşme, işbu Sözleşme ve hizmetin işlevlerinin Müşteri tarafından kullanılmasıdır (özellikle yükleme, transkripsiyon, değerlendirme, düzenleme, paylaşma, dışa aktarma ve silme). Bir işlevin her kullanımı, ilgili işlemenin gerçekleştirilmesine yönelik belgelenmiş bir münferit talimattır.

3.2 Müşteri diğer talimatları yazılı olarak verir; datenschutz@scryp.at adresine e-posta gönderilmesi yeterlidir. Talimat vermeye hesap sahibi ve Müşterinin scryp hesabı için görevlendirdiği kişiler yetkilidir. Hizmetin kapsamını aşan talimatlar, hizmet değişikliği başvurusu olarak kabul edilir.

3.3 Bir talimatın scryp'in görüşüne göre GDPR'yi veya diğer veri koruma hükümlerini ihlal etmesi hâlinde scryp, Müşteriyi derhâl bilgilendirir. scryp, Müşteri talimatı teyit edene veya değiştirene kadar talimatın uygulanmasını askıya alabilir.

3.4 scryp verileri kendi amaçları için kullanmaz. Özellikle Müşterinin kayıtları, transkriptleri ve değerlendirmeleri yapay zekâ modellerinin eğitimi veya iyileştirilmesi için kullanılmaz ve işbu Sözleşmede aksi öngörülmedikçe üçüncü kişilere aktarılmaz.

3.5 Bir makamın veya mahkemenin scryp'ten Müşterinin verilerinin teslim edilmesini talep etmesi hâlinde scryp, hukuken izin verildiği ölçüde Müşteriyi derhâl bilgilendirir, ilgili merciyi Müşteriye yönlendirir ve yalnızca yasal olarak yükümlü olduğu verileri teslim eder. scryp bu sırada, Müşterinin yasal bir sır saklama yükümlülüğünün teslime engel olup olmadığını inceler (§ 6(5) DSG).

4. Müşterinin yükümlülükleri

4.1 Müşteri, kayıtların ve bunların işlenmesinin hukuka uygunluğundan sorumludur. Müşteri özellikle bir hukuki dayanağın bulunmasını (GDPR Madde 6, özel nitelikli kategoriler için GDPR Madde 9), ilgili kişilerin bilgilendirilmesini (GDPR Madde 13 ve 14) ve aleni olmayan hiçbir ifadenin konuşanların rızası olmaksızın kaydedilmemesini sağlar (örneğin Avusturya'da § 120 StGB).

4.2 Kayıtların özel nitelikli kişisel veri kategorileri (örneğin sağlık verileri) veya meslek sırrına tabi içerikler içermesi hâlinde Müşteri, işlemeye izin verilip verilmediğini ve bir veri koruma etki değerlendirmesinin (GDPR Madde 35) gerekli olup olmadığını önceden inceler. scryp bunun için işbu Sözleşmede ve eklerinde yer alan bilgileri sağlar.

4.3 Müşteri, scryp hesabının e-posta adresini güncel tutar. scryp, işbu Sözleşme kapsamındaki tüm bildirimleri, özellikle Madde 10 uyarınca yapılacak bildirimleri bu adrese gönderir.

4.4 Müşteri, scryp'e talimat verme, kanıt talep etme ve Madde 11 uyarınca denetim yapma hakkına sahiptir.

5. Gizlilik ve meslek sırrı

5.1 scryp, verilere erişimi yalnızca veri gizliliği (§ 6 DSG) ve sır saklama yükümlülüğü altına alınmış ve ihlalin sonuçları hakkında bilgilendirilmiş kişilere tanır (GDPR Madde 28(3)(b), Madde 29). Bu yükümlülük, faaliyetin sona ermesinden sonra da devam eder.

5.2 scryp, Müşterinin içeriklerinin (kayıtlar, transkriptler, değerlendirmeler, dosya ve klasör adları) yalnızca şifreli olarak saklanacağı ve düz metin olarak yalnızca ilgili işlemenin süresi boyunca işleme sunucularının belleğinde (RAM) bulunacağı şekilde tasarlanmıştır. scryp'teki kişiler, olağan işletim sırasında düz metin içeriklere erişemez. Ayrıntılar Ek 2'de yer almaktadır.

5.3 Müşterinin yasal bir sır saklama yükümlülüğüne tabi olması hâlinde (örneğin § 9 RAO, § 54 ÄrzteG, § 121 StGB) scryp, Müşterinin yardımcısı sıfatıyla, hizmet kapsamında erişebildiği tüm içerikleri aynı şekilde gizli tutmayı taahhüt eder. Alman hukukuna tabi müşteriler için bu taahhüt, aynı zamanda § 203(4) StGB (Almanya) uyarınca sır saklama yükümlülüğü olarak geçerlidir. Talep hâlinde scryp bu taahhüdü ayrı bir beyanla teyit eder.

6. İşlemenin güvenliği

6.1 scryp, GDPR Madde 32 uyarınca Ek 2'de açıklanan teknik ve organizasyonel önlemleri alır.

6.2 scryp bu önlemleri geliştirebilir ve eşdeğer veya daha iyi önlemlerle değiştirebilir. Bu sırada koruma düzeyinin altına inilemez. scryp, önemli değişiklikleri belgeler ve Müşteriye bildirir. Ek 2'nin güncel sürümüne www.scryp.at/avv adresinden ulaşılabilir.

6.3 scryp, önlemlerin etkinliğini en az yılda bir kez gözden geçirir ve sonucu talep üzerine Müşteriye bildirir.

7. Alt veri işleyenler

7.1 Müşteri, Ek 3'te belirtilen alt veri işleyenleri onaylar (GDPR Madde 28(2) uyarınca genel izin).

7.2 scryp'in bir alt veri işleyen eklemek veya değiştirmek istemesi hâlinde scryp, Müşteriyi kullanıma başlamadan en az 30 gün önce scryp hesabının adresine e-posta göndererek bilgilendirir. Müşteri, bu bildirimin ulaşmasından itibaren 14 gün içinde veri koruma hukukuna ilişkin haklı bir nedenle yazılı olarak itiraz edebilir; e-posta yeterlidir. Müşterinin itiraz etmemesi hâlinde değişiklik onaylanmış sayılır.

7.3 Tarafların bir itirazın ardından çözüm bulamaması hâlinde Müşteri, Ana Sözleşmeyi planlanan kullanımın başlangıç tarihi itibarıyla feshedebilir. Müşterinin fesihten sonraki dönem için peşin ödediği ücretleri scryp orantılı olarak iade eder.

7.4 scryp, her alt veri işleyene, işbu Sözleşme uyarınca scryp'in tabi olduğu veri koruma yükümlülüklerinin aynısını, özellikle uygun teknik ve organizasyonel önlemlere ilişkin yeterli güvenceleri sözleşmeyle yükler (GDPR Madde 28(4)). Bir alt veri işleyenin yükümlülüklerini yerine getirmemesi hâlinde scryp, Müşteriye karşı alt veri işleyenin yükümlülüklerinden kendi davranışından sorumlu olduğu gibi sorumludur.

7.5 Müşteri verilerine erişim içermeyen yan hizmetler, örneğin telekomünikasyon, temizlik veya veri erişimi olmaksızın bakım, alt veri işleme sayılmaz.

8. İşleme yeri ve üçüncü ülkeler

8.1 scryp verileri Avusturya ve Almanya'da işler ve saklar. scryp tarafından Avrupa Birliği veya Avrupa Ekonomik Alanı dışındaki ülkelere veri aktarımı yapılmaz.

8.2 Bir alt veri işleyenin verileri üçüncü bir ülkede işlemesi hâlinde bu işleme, yalnızca Ek 3'te açıklanan kapsamda ve yalnızca GDPR Bölüm V uyarınca uygun bir güvenceyle (örneğin AB Komisyonu'nun yeterlilik kararı veya AB Standart Sözleşme Maddeleri) gerçekleştirilir.

9. Müşteriye destek

9.1 İlgili kişilerin hakları: Müşteri; erişim, düzeltme, silme ve veri taşınabilirliği taleplerini çoğu durumda hizmetin işlevleri (görüntüleme, düzenleme, dışa aktarma, silme) aracılığıyla kendisi yerine getirebilir. scryp içerikleri yalnızca şifreli olarak tuttuğundan, bir kayıtta hangi kişilerin yer aldığını tespit edemez. Bir ilgili kişinin scryp'e başvurması hâlinde scryp, talebi derhâl Müşteriye iletir ve Müşteri aksi yönde talimat vermedikçe talebi kendisi yanıtlamaz.

9.2 Güvenlik, kişisel veri ihlalleri, veri koruma etki değerlendirmesi ve denetim makamına danışma (GDPR Madde 32 ila 36): scryp, Müşteriyi elinde bulunan bilgilerle, özellikle işbu Sözleşme, Ek 2 ve Madde 10 uyarınca bir olaya ilişkin bilgilerle destekler.

9.3 İşbu Sözleşmede açıklanan bilgi ve işlevlerin sağlanmasının ötesine geçen destek için scryp, önceden bildirmek kaydıyla harcanan çabaya göre makul bir ücret talep edebilir. Desteğin scryp'in bir hatası nedeniyle gerekli olması hâlinde bu hüküm uygulanmaz.

10. Kişisel veri ihlallerinin bildirilmesi

10.1 scryp'in, Müşterinin verilerini etkileyen bir kişisel veri ihlalinden haberdar olması hâlinde scryp bunu, gereksiz gecikme olmaksızın ve en geç öğrenmesinden itibaren 48 saat içinde, scryp hesabının adresine e-posta göndererek Müşteriye bildirir.

10.2 Bildirim, bilindiği ölçüde şunları içerir: ihlalin niteliği, etkilenen veri türleri ve etkilenen kişilerin yaklaşık sayısı, olası sonuçlar, alınan ve önerilen önlemler ile scryp'te bir iletişim noktası. Henüz mevcut olmayan bilgileri scryp, gereksiz gecikme olmaksızın sonradan iletir.

10.3 scryp ihlali belgeler ve Müşteriyi denetim makamına yapılacak bildirimde ve ilgili kişilerin bilgilendirilmesinde destekler. scryp, Müşteri adına makamlara veya ilgili kişilere bildirimleri yalnızca Müşterinin talimatı üzerine yapar. Müşteriye yapılan bildirim, kusurun kabulü anlamına gelmez.

11. Kanıtlar ve denetimler

11.1 scryp, GDPR Madde 28'den doğan yükümlülüklere uyulduğunun kanıtlanması için gerekli tüm bilgileri Müşteriye sunar. Bunlar arasında işbu Sözleşme, Ek 2'deki önlemlerin açıklaması, GDPR Madde 30(2) uyarınca tutulan kayıt, alt veri işleyenlerin sertifikaları ve Müşterinin gerekçeli sorularına verilen yazılı yanıtlar yer alır.

11.2 Bu kanıtların münferit durumda yeterli olmaması hâlinde Müşteri, kendisi veya sır saklama yükümlülüğü altına alınmış ve scryp'in rakibi olmayan bir denetçi aracılığıyla, yerinde inceleme dâhil bir denetim gerçekleştirebilir. Denetimler, takvim yılı başına en fazla bir kez, en az 30 gün önceden bildirimde bulunularak, olağan çalışma saatleri içinde ve işletimi aksatmadan yapılır. Bir ihlale ilişkin somut belirtilerin bulunması veya bir denetim makamının talep etmesi hâlinde denetim kısa süre içinde ve daha sık da yapılabilir.

11.3 Denetim, diğer müşterilerin verilerini ve alt veri işleyenlerin veri merkezlerini kapsamaz. Bunlar için alt veri işleyenlerin sertifikaları ve denetim raporları geçerlidir. Her Taraf, denetime ilişkin kendi masraflarını üstlenir.

12. Verilerin silinmesi ve iadesi

12.1 Sözleşme süresi boyunca Müşteri, verilerini dilediği zaman kendisi silebilir ve yaygın biçimlerde dışa aktarabilir. Silinen içerikler etkin veri kümesinden derhâl kaldırılır.

12.2 Yüklenen özgün dosyaları scryp, işlemenin tamamlanmasının ardından, kural olarak birkaç dakika içinde ve en geç yüklemeden 72 saat sonra otomatik olarak siler. Yalnızca şifreli oynatma sürümü, şifreli transkript ve şifreli değerlendirmeler saklanmaya devam eder.

12.3 Ana Sözleşmenin sona ermesinden sonra içerikler, dışa aktarım için Müşteriye 90 güne kadar sunulmaya devam eder. Bunun ardından scryp içerikleri tüm kopyaları dâhil otomatik olarak siler. Müşterinin hesabını silmesi hâlinde tüm veriler derhâl silinir.

12.4 Yedek kopyalar yalnızca sistemin bütününün geri yüklenmesine hizmet eder. Yedek kopyalar Müşterinin içeriklerini yalnızca şifreli olarak içerir ve en geç 30 gün sonra üzerlerine yazılır. Silinen münferit müşteri verileri yedek kopyalardan geri yüklenmez.

12.5 scryp'in yasal saklama yükümlülükleri nedeniyle saklamaya devam etmek zorunda olduğu veriler (örneğin § 132 BAO uyarınca fatura verileri) silme kapsamı dışındadır. Bu veriler erişime kapatılır ve sürenin dolmasının ardından silinir.

12.6 Talep üzerine scryp, silme işlemini yazılı olarak teyit eder; e-posta yeterlidir.

13. Sorumluluk

13.1 İlgili kişilere karşı Taraflar, GDPR Madde 82 uyarınca sorumludur.

13.2 Tarafların birbirlerine karşı ilişkisinde, hukuken izin verildiği ölçüde Ana Sözleşmenin sorumluluk hükümleri geçerlidir. Alt veri işleyenlerden scryp, kendi davranışından sorumlu olduğu gibi sorumludur (Madde 7.4).

13.3 Bir Tarafın ilgili kişilere tazminat ödemiş olması hâlinde bu Taraf, diğer Taraftan, zarara ilişkin sorumluluktaki payına karşılık gelen kısmı geri talep edebilir (GDPR Madde 82(5)).

13.4 Müşterinin, scryp'in Madde 3.3 uyarınca hukuka aykırılığına işaret etmesine rağmen bir talimatı sürdürmesi hâlinde Müşteri, bu talimata dayanan tüm üçüncü kişi talepleri ve idari para cezaları bakımından scryp'i sorumluluktan kurtarır ve bunları üstlenir.

14. Süre, askıya alma ve sona erme

14.1 İşbu Sözleşme, scryp Müşteri için veri işlediği sürece, yani Ana Sözleşmenin süresi boyunca ve Madde 12 uyarınca silme işlemi tamamlanana kadar geçerlidir.

14.2 Madde 1.4 kapsamındaki müşteriler için hizmetin işbu Sözleşme olmaksızın kullanılması öngörülmemiştir. Bu nedenle işbu Sözleşmenin feshi, aynı zamanda Ana Sözleşmenin feshi olarak da geçerlidir.

14.3 scryp'in işbu Sözleşmeyi ihlal etmesi hâlinde Müşteri, ihlal giderilene kadar scryp'in ilgili işlemeyi askıya almasını talep edebilir. scryp'in önemli bir ihlali, talepten itibaren bir ay içinde gidermemesi hâlinde Müşteri, Ana Sözleşmeyi bildirim süresi olmaksızın feshedebilir.

15. Son hükümler

15.1 İşbu Sözleşme elektronik biçimde akdedilir (GDPR Madde 28(9)). Madde 1.4 kapsamındaki müşteriler için işbu Sözleşme, Hizmet Koşulları'na dâhil edilmek suretiyle Ana Sözleşmenin akdedilmesiyle sözleşmenin bir parçası hâline gelir; bu durumda sözleşme tarafı, hesapta kayıtlı bilgileriyle scryp hesabının sahibidir. Bunun yanı sıra işbu Sözleşme, elektronik kopya olarak da dâhil olmak üzere, bu belgenin her iki Tarafça imzalanmasıyla akdedilebilir.

15.2 İşbu Sözleşmede yapılacak değişiklikler yazılı şekle tabidir; e-posta yeterlidir. scryp, Ek 2'yi Madde 6.2 ve Ek 3'ü Madde 7.2 uyarınca uyarlayabilir. Diğer değişiklikleri scryp, yürürlüğe girmeden en az 30 gün önce e-posta ile duyurur; Müşteri bu tarihe kadar itiraz edebilir ve Ana Sözleşmeyi bu tarih itibarıyla feshedebilir. scryp, işbu Sözleşmenin her sürümünü sürüm numarası ve tarihiyle birlikte muhafaza eder.

15.3 Avusturya hukuku uygulanır; GDPR hükümleri saklıdır. Müşterinin tacir olması hâlinde işbu Sözleşmeden doğan tüm uyuşmazlıklar için Viyana'daki görevli mahkeme münhasıran yetkilidir. Emredici yasal yetki kuralları saklıdır.

15.4 Bir hükmün geçersiz olması hâlinde Sözleşmenin geri kalanı geçerliliğini korur. Geçersiz hükmün yerine, amacına en yakın yasal düzenleme geçer.

15.5 İşbu Sözleşmeye ilişkin tüm sorular için scryp tarafındaki iletişim noktası datenschutz@scryp.at adresidir. Müşteri tarafında ise, Müşteri aksini bildirmedikçe, scryp hesabının e-posta adresidir.

15.6 scryp, işbu Sözleşmeyi birden fazla dilde sunar. Bağlayıcı olan Almanca sürümdür; çeviriler anlaşılmasına yardımcı olmak amacıyla sunulur. Farklılık hâlinde Almanca metin geçerlidir.

İmzalar

Müşteri adına	**scryp adına**
Yer, tarih	Yer, tarih
Ad, görev	Gökhan Sagir, şahıs işletmesi sahibi
İmza	İmza

Ek 1: İşlemenin tanımı

Başlık	Açıklama
Konu	scryp hizmetinin sunulması: konuşma tanıma ve konuşmacı tanıma ile ses ve video kayıtlarının transkripsiyonu, Ultra planında ek olarak yapay zekâ özellikleri (yapay zekâ destekli değerlendirme: özet, tutanak, görev listesi, sosyal medya metni) ile sonuçların saklanması, düzenlenmesi, dışa aktarılması ve paylaşılması.
Amaç	Müşteri, kendi kayıtlarını, örneğin toplantıları, röportajları, dikteleri, danışmanlık görüşmelerini, sunumları veya podcast'leri metne dönüştürtür ve değerlendirtir.
İşlemenin niteliği	Şifreli dosyaların alınması, işleme sunucularının belleğinde (RAM) kısa süreli şifre çözme, otomatik transkripsiyon ve değerlendirme, sonuçların şifrelenmesi, şifreli saklama, Müşterinin hesabında sunulması, silme.
Veri türleri	Ses kayıtları ve videolar (ses, konuşulan içerikler), bunlardan üretilen transkriptler ve değerlendirmeler, konuşmacı atamaları, Müşteri tarafından verilen dosya ve klasör adları, teknik meta veriler (süre, dosya boyutu, zaman bilgileri, tanınan dil, işleme durumu), paylaşılan transkriptlerde paylaşım bağlantısı. Tüm içerikler şifreli olarak saklanır; yalnızca teknik meta veriler düz metin olarak bulunur.
Özel nitelikli kategoriler (GDPR Madde 9)	Müşterinin kayıtlarının içeriğine bağlı olarak mümkündür (örneğin hekim diktelerindeki sağlık verileri, danışmanlık veya müvekkil görüşmelerindeki bilgiler). scryp içeriği bilmez. İzin verilip verilmediğini Müşteri, Madde 4.2 uyarınca inceler.
Özel nitelikli kategoriler için güvenceler	Müşterinin tarayıcısında şifreleme, düz metnin yalnızca scryp'in Viyana'daki kendi sunucularının belleğinde bulunması, içeriklerin alt veri işleyenlere düz metin olarak aktarılmaması, olağan işletim sırasında kişilerin içeriklere erişememesi, Madde 5 uyarınca sır saklama yükümlülüğü, müşteri verileriyle yapay zekâ modeli eğitimi yapılmaması.
İlgili kişiler	Kayıtlarda konuşan veya adı geçen kişiler (örneğin çalışanlar, müşteriler, hastalar, müvekkiller, röportaj yapılan kişiler, toplantı ve etkinlik katılımcıları) ile Müşteri hesabının kullanıcıları.
İşleme yerleri	Transkripsiyon ve yapay zekâ değerlendirmesi: scryp'in Viyana, Avusturya'daki kendi GPU sunucuları. Web uygulaması, arayüzler, veritabanı, şifreli dosya depolama ve yedek kopyalar: Hetzner Online GmbH'nin Nürnberg, Almanya'daki veri merkezi.
Süre	Ana Sözleşmenin süresi ile Madde 12 uyarınca silme süreleri.

Ek 2: Teknik ve organizasyonel önlemler (GDPR Madde 32)

Son güncelleme: 22 Eylül 2026. Önlemler, scryp'in olağan işletimini tanımlar.

1. Şifreleme ve sıfır bilgi (zero-knowledge) mimarisi

- Kayıtlar, scryp'e aktarılmadan önce Müşterinin tarayıcısında AES-256-GCM ile şifrelenir. Her dosya için ayrı bir dosya anahtarı (FEK) oluşturulur.
- Dosya anahtarları, hesabın ana anahtarıyla (MEK) şifrelenir. Ana anahtara yalnızca Müşterinin parolasıyla erişilebilir (PBKDF2-SHA256 ile türetme, 600.000 yineleme). scryp, ne parolayı ne de ana anahtarı düz metin olarak bilir.
- Transkripsiyon için tarayıcı, dosya anahtarını bir sunucu anahtarıyla (RSA-4096, OAEP) şifreleyerek scryp'e iletir. İşleme sunucusu, kaydın şifresini yalnızca bellekte (RAM) çözer. Geçici dosyalar bir RAM dosya sisteminde bulunur ve iş tamamlandıktan sonra atılır; şifrelenmemiş içerikler hiçbir zaman veri depolama ortamına yazılmaz.
- Transkriptler ve değerlendirmeler, oluşturulduktan hemen sonra dosya anahtarıyla şifrelenir ve yalnızca şifreli olarak saklanır. Dosya ve klasör adları tarayıcıda şifrelenir.
- Bir transkript paylaşılırken dosya anahtarı, paylaşım parolasından türetilen bir anahtarla şifrelenir. Alıcılar şifreyi yalnızca kendi tarayıcılarında çözer.
- URL ile yükleme istisnası: Müşterinin bir kaydı bir internet adresi üzerinden alması hâlinde işleme sunucusu dosyayı doğrudan indirir, bellekte işler ve ardından siler; transkript ve oynatma sürümü her zamanki gibi şifreli olarak saklanır.
- Tüm bağlantılar TLS 1.2 veya 1.3 ile şifrelenir.

2. Fiziksel erişim kontrolü

- Web uygulaması, veritabanı, dosya depolama ve yedek kopyalar, Hetzner Online GmbH'nin Nürnberg'deki veri merkezinde (ISO/IEC 27001 sertifikalı, BSI C5 Tip 2 tasdikli) işletmecinin giriş kontrolü, video gözetimi ve güvenlik personeli korumasında çalışır.
- Transkripsiyon ve yapay zekâ değerlendirmesi için kullanılan GPU sunucuları, scryp'in Viyana'daki kendi kapalı odalarında bulunur. Yalnızca yetkili kişiler girebilir; giriş mekanik olarak kilitlidir ve ek olarak biyometrik yöntemle güvence altına alınmıştır.
- Bu sunucuların tüm veri depolama ortamları tamamen şifrelidir. Bir veri depolama ortamının çalınması veya sökülmesi hâlinde veriler anahtar olmadan okunamaz. Şifrelenmemiş içerikler bu sunucularda yalnızca devam eden bir iş sırasında bellekte bulunur ve hiçbir zaman veri depolama ortamına yazılmaz.

3. Sisteme erişim ve veri erişimi kontrolü

- Sunucu erişimi yalnızca scryp yöneticileri için, kişisel anahtarlar veya rastgele oluşturulmuş güçlü parolalarla şifreli SSH bağlantıları üzerinden; erişim en az ayrıcalık ilkesine göre.
- Kendi oturum açma sistemine sahip ve onaylı IP adresleriyle sınırlı ayrı yönetim arayüzü. Yönetim arayüzü yalnızca hesap ve iş meta verilerini gösterir, içerik göstermez.
- Kullanıcı hesapları: Parolalar Argon2id ile karmalanır; oturum açma denemelerine karşı hız sınırlaması ve geçici kilitleme ile koruma; oturumlar çerez olmadan kısa ömürlü token'larla yürütülür.
- Arayüzlerin kötüye kullanıma ve aşırı yüke karşı hız sınırlaması ve otomatik engellemelerle korunması.
- Otomatik hizmetler (işleme sunucuları), kendilerine ait ve döndürülebilir erişim bilgileriyle kimlik doğrulaması yapar ve yalnızca ilgili iş için gerekli anahtarları alır.

4. Ayırma kontrolü ve takma adlandırma

- Kriptografik ayırma: Her müşterinin kendi ana anahtarı, her dosyanın kendi dosya anahtarı vardır. Bir müşterinin içerikleri başka anahtarlarla okunamaz.
- Üretim, veritabanı, önbellek ve izleme sistemlerinin ayrı ağ bölgelerinde mantıksal olarak ayrılması.
- GPU sunucularına gönderilen işleme işleri ad ve e-posta adresi içermez; yalnızca iş için gerekli teknik verileri içerir.

5. Bütünlük ve izlenebilirlik

- Uygulama ve altyapıdaki tüm değişiklikler sürüm kontrollü kaynak kodu ve otomatik, izlenebilir dağıtım üzerinden yapılır; yazılım imajları sağlama toplamlarıyla sabitlenir.
- Hesap olayları (örneğin oturum açma, silme, abonelik değişiklikleri) IP adresi olmaksızın zaman bilgisiyle kaydedilir.
- Sistem günlükleri içerik içermez ve 14 gün sonra silinir. IP adresleri saklanmaz ve günlüğe kaydedilmez. Kötüye kullanımın önlenmesi için erişimler yalnızca kısa ömürlü, gizli bir anahtarla oluşturulan ve geri hesaplanamayan bir takma ad üzerinden sayılır; bu takma ad en geç bir saat sonra geçerliliğini yitirir.

6. Erişilebilirlik ve dayanıklılık

- Yük dağıtımlı üç sunucudan oluşan yüksek erişilebilirlikli küme; üç düğüme eş zamanlı çoğaltma yapan veritabanı; otomatik yük devretmeli önbellek.
- Son 30 gün içindeki herhangi bir zamana geri yükleme imkânıyla veritabanının günlük şifreli yedeklenmesi; küme yapılandırması altı saatte bir yedeklenir. Yedekler Nürnberg'deki veri merkezinde bulunur.
- Yeni sürümlerin işletim kesintisi olmaksızın dağıtılması; ağ ve uygulama katmanında aşırı yük saldırılarına karşı koruma.
- Arızalarda otomatik uyarı veren sürekli izleme.

7. Silme ve veri minimizasyonu

- Yüklenen özgün dosyalar işlemeden sonra, kural olarak birkaç dakika içinde silinir; otomatik bir kural, askıda kalan yüklemeleri en geç 72 saat sonra kaldırır.
- Müşteri, içeriklerini ve hesabını dilediği zaman kendisi siler; silme, etkin veri kümesinde derhâl etkili olur. Bir aboneliğin sona ermesinden sonra içerikler 90 gün sonra otomatik olarak silinir.
- Çerez yok, üçüncü taraf izleme veya analiz aracı yok, IP adresi saklama yok.

8. Organizasyon

- scryp'te görev yapan tüm kişiler veri gizliliği ve sır saklama yükümlülüğü altına alınmış ve güvenlik mimarisi hakkında bilgilendirilmiştir.
- scryp, veri işleme faaliyetleri kaydı tutar (GDPR Madde 30). Veri koruma etki değerlendirmesi, kayıt ve bu önlemler en az yılda bir kez ve önemli değişikliklerde gözden geçirilir.
- Olay süreci: izleme yoluyla tespit, değerlendirme, sınırlama, Sözleşmenin Madde 10'u uyarınca etkilenen müşterilere bildirim, sonradan değerlendirme.
- Alt veri işleyenler, kullanılmadan önce güvenceleri bakımından incelenir ve GDPR Madde 28(4) uyarınca sözleşmeyle yükümlü kılınır.

Ek 3: Alt veri işleyenler

Son güncelleme: 22 Eylül 2026.

Alt veri işleyen	Hizmet	Veriler	İşleme yeri	Güvence
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Almanya	Web uygulaması, arayüzler ve veritabanı için sunucuların işletilmesi; şifreli nesne depolama; yedek kopyalar	Ek 1'de belirtilen tüm veriler, içerikler yalnızca şifreli	Nürnberg, Almanya (AB)	Veri işleme sözleşmesi; ISO/IEC 27001; BSI C5
Mailjet GmbH (Sinch-Konzern), Alt Moabit 2, 10557 Berlin, Almanya	Sistem e-postalarının gönderilmesi (örneğin “Transkript hazır” bildirimi)	Hesabın e-posta adresi, işin tarihi, hesaba bağlantı; içerik yok, dosya adı yok	Fransa (AB)	Veri işleme sözleşmesi; ISO/IEC 27001
Microsoft Ireland Operations Ltd., Dublin, İrlanda	Destek taleplerinin e-posta yoluyla alınması ve işlenmesi (Microsoft 365)	Yalnızca Müşterinin bir destek talebinde kendisinin ilettiği veriler	AB; üçüncü ülkelerden uzaktan erişim mümkün	Veri işleme sözleşmesi; AB Standart Sözleşme Maddeleri; AB-ABD Veri Gizliliği Çerçevesi