SON GÜNCELLEME: 22 EKİM 2026

Veri İşleme Sözleşmesi

Bu Veri İşleme Sözleşmesi (“Sözleşme”), Groupshift Bilişim Teknolojileri ve Yazılım Hizmetleri Sanayi ve Ticaret Ltd. Şti. (“LyngL”, “biz”) ile LyngL’i Kullanım Koşulları kapsamında kullanan işletme (“Müşteri”, “siz”) arasındadır. Kullanım Koşulları’nın parçasıdır ve LyngL’in Müşteri adına kişisel veri işlediği her durumda uygulanır.

İndir: Veri İşleme Sözleşmesi (PDF). İmzalı bir kopya isterseniz info@lyngl.com adresine yazın.

---

1. Tanımlar

- “Kişisel veri”, “işleme”, “veri sorumlusu” ve “veri işleyen” ifadeleri, 6698 sayılı Kişisel Verilerin Korunması Kanunu’nda (“KVKK”) ve uygulandığı durumlarda AB Genel Veri Koruma Tüzüğü’nde (“GDPR”) verilen anlamları taşır.
- “Müşteri Kişisel Verisi”, Müşteri’nin veya kullanıcılarının LyngL’e koyduğu ya da LyngL’in Müşteri’nin bağladığı hizmetlerden aldığı ve Müşteri adına işlediği kişisel verilerdir.
- “Alt işleyen”, LyngL’in Müşteri Kişisel Verisini işlemek için görevlendirdiği üçüncü kişidir.
- “Güvenlik Sayfası”, Güvenlik ve KVKK sayfamızdır.

2. Roller ve kapsam

Müşteri Kişisel Verisi bakımından Müşteri veri sorumlusu, LyngL veri işleyendir. Bu Sözleşme, Müşteri’nin hesap ve fatura bilgileri gibi LyngL’in veri sorumlusu olarak işlediği kişisel verileri kapsamaz; bunlar Gizlilik Politikası kapsamındadır.

İşlemenin konusu, niteliği, amacı ve süresi ile kişisel veri ve ilgili kişi kategorileri Ek 1’de açıklanmıştır.

3. Müşteri’nin talimatları

LyngL, Müşteri Kişisel Verisini yalnızca Müşteri’nin belgelenmiş talimatlarıyla işler. Müşteri’nin LyngL’i kullanması (Yönetici’ye verdiği hedefler, seçtiği ayarlar, onayladığı işlemler ve bağladığı hizmetler) ve bu Sözleşme, Müşteri’nin talimatlarıdır. LyngL bir talimatın KVKK’ya veya GDPR’a aykırı olduğunu düşünürse Müşteri’yi bilgilendirir.

Müşteri, LyngL'e koyduğu kişisel veriler için hukuki bir dayanağı olmasından, ilgili kişileri aydınlatmaktan ve gerekiyorsa açık rızalarını almaktan ve özel nitelikli kişisel verileri LyngL'e yalnızca gerekli ve hukuka uygun olduğu durumlarda koymaktan sorumludur.

4. LyngL'in yükümlülükleri

LyngL:

- Müşteri Kişisel Verisini yalnızca hizmeti sunmak için ve talimatlara uygun olarak işler, satmaz ve yapay zekâ modellerini eğitmek için kullanmaz;
- bu verilere erişebilen çalışanlarının gizlilik yükümlülüğü altında olmasını ve verilere yalnızca destek, güvenlik veya kalite kontrolü için gerektiğinde erişmesini sağlar; her erişim kayda geçer;
- Ek 2'deki teknik ve idari tedbirleri uygular ve en az bu seviyede tutar;
- Müşteri'ye, ilgili kişilerin KVKK'nın 11. maddesi veya GDPR kapsamındaki haklarını kullandıkları başvuruları yanıtlamasında ve güvenlik, ihlal bildirimi ve etki değerlendirmelerinde makul ölçüde yardımcı olur;
- Müşteri Kişisel Verisiyle ilgili olarak bir ilgili kişiden doğrudan aldığı başvuruyu Müşteri'ye iletir ve Müşteri yetki vermedikçe kendisi yanıtlamaz;
- bu Sözleşme'ye uyumu göstermek için gereken bilgileri Müşteri'ye verir.

5. Alt işleyenler

Müşteri, LyngL'in Güvenlik Sayfası'nda listelenen alt işleyenleri kullanmasına izin verir. LyngL her alt işleyene Müşteri Kişisel Verisini en az bu Sözleşme kadar koruyan veri koruma yükümlülükleri yükler ve onların yükümlülüklerini yerine getirmesinden Müşteri'ye karşı sorumlu kalır.

LyngL yeni bir alt işleyeni, Müşteri Kişisel Verisini işlemeye başlamadan en az 15 gün önce Güvenlik Sayfası'nda duyurur. Müşteri bu süre içinde makul veri koruma gerekçeleriyle yazılı olarak itiraz edebilir. İtiraz çözülemezse Müşteri hizmetin etkilenen bölümünü sona erdirebilir ve o bölüm için peşin ödediği ücretin kalan süreye düşen kısmını geri alır.

6. Yurt dışına aktarım

LyngL'in alt işleyenleri Müşteri Kişisel Verisini Türkiye dışında, Güvenlik Sayfası'nda belirtilen yerlerde işler. LyngL bu aktarımları KVKK'nın 9. maddesine ve GDPR'ın uygulandığı durumlarda V. bölümüne uygun olarak, öngördükleri güvencelerle yapar.

7. Güvenlik ihlalleri

LyngL, Müşteri Kişisel Verisinin kazara veya hukuka aykırı olarak yok edilmesine, kaybolmasına, değiştirilmesine ya da yetkisiz olarak ifşa edilmesine veya erişilmesine yol açan bir güvenlik ihlalini öğrenirse, Müşteri'ye gecikmeksizin ve en geç 72 saat içinde bildirir ve Müşteri'nin Kişisel Verileri Koruma Kurulu'na bildirim dahil kendi yükümlülüklerini yerine getirmesi için makul olarak ihtiyaç duyduğu bilgileri verir.

LyngL ihlali sınırlamak ve etkilerini azaltmak için makul önlemleri alır ve Müşteri'yi bilgilendirmeye devam eder.

8. Denetim

LyngL, talep üzerine yazılı güvenlik sorularını yanıtlar ve Ek 2'deki tedbirlerin belgelerini sunar. Bunlar uyumu göstermeye yetmezse Müşteri, yılda en fazla bir kez ve 30 gün önceden bildirerek, masrafı kendisine ait olmak üzere gizlilik yükümlülüğü altındaki bağımsız bir denetçiye, mesai saatlerinde ve hizmeti aksatmadan ya da diğer müşterilerin verilerini açığa çıkarmadan denetim yaptırabilir. Yetkili makamların denetimleri bu sınırlamalara tabi değildir.

9. İade ve silme

Müşteri, hesabı açık olduğu sürece içeriğini dışa aktarabilir, örneğin proje dosyalarını indirebilir. Müşteri bir çalışma alanını veya hesabını sildiğinde ya da Kullanım Koşulları sona erdiğinde LyngL, mevzuat bir kısmını saklamasını gerektirmedikçe Müşteri Kişisel Verisini 30 gün içinde siler.

Şifreli veritabanı yedekleri en fazla 400 gün saklanır ve sonra silinir. O zamana kadar yedeklerdeki silinmiş veriler kullanılmaz ve Ek 2'de anlatıldığı şekilde korunur.

10. Sorumluluk

Tarafların bu Sözleşme kapsamındaki sorumluluğu, mevzuatın sınırlamaya izin vermediği durumlar dışında, Kullanım Koşulları'ndaki sınırlamalara tabidir.

11. Süre, öncelik ve uygulanacak hukuk

Bu Sözleşme, LyngL Müşteri Kişisel Verisini işlediği sürece geçerlidir. Kişisel verilerin korunması konusunda Kullanım Koşulları ile çelişirse bu Sözleşme önceliklidir. Mevzuat veya hizmetimiz değiştiğinde Sözleşme'yi güncelleyebiliriz; yeni sürümü tarihiyle bu sayfada yayınlar, önemli değişiklikleri Müşterilere önceden bildiririz.

Bu Sözleşme Türkiye Cumhuriyeti hukukuna tabidir. Uyuşmazlıklarda İzmir mahkemeleri ve icra daireleri yetkilidir.

12. Ek 1: İşlemenin ayrıntıları

- Konu ve amaç: LyngL'in sunulması, yani Müşteri'nin istediği işlerin (araştırma ve raporlar, içerik, görsel ve video, yayınlama, reklam, yazılım ve tekrarlayan işler) yapay zekâ çalışanlarıyla planlanması ve yapılması.
- Nitelik: toplama, saklama, düzenleme, erişme, analiz, işin gerektirdiği sağlayıcılara aktarma, yeni içerik üretme ve silme.
- Süre: Müşteri LyngL'i kullandığı sürece ve 9. bölümdeki silme süreleri boyunca.
- İlgili kişiler: Müşteri'nin kullanıcıları ile verileri Müşteri tarafından LyngL'e konulan ya da LyngL'in bağlı hizmetlerden aldığı kişiler; örneğin Müşteri'nin müşterileri, potansiyel müşterileri, çalışanları, adayları, tedarikçileri ve sosyal medya takipçileri.
- Kişisel veri kategorileri: kimlik ve iletişim bilgileri, mesajlar ve e-postalar, içerik ve dosyalar, kullanıcı adları ve yorumlar gibi sosyal medya verileri, reklam sonuçları ve Müşteri'nin LyngL'e koymayı seçtiği diğer veriler.
- Özel nitelikli kişisel veriler: yalnızca Müşteri bunları kendi hukuki dayanağıyla LyngL'e koyarsa.

13. Ek 2: Teknik ve idari tedbirler

- Her bağlantıda aktarım sırasında şifreleme (TLS); API anahtarları ve erişim jetonları AES-256-GCM ile şifreli; parolalar yalnızca tek yönlü özet olarak saklanır; veritabanı yedekleri saklanmadan önce AES-256-GCM ile şifrelenir; dosyalar depolama sağlayıcısında şifreli durur.
- Her çalışma alanının verilerinin mantıksal olarak ayrılması; her sorgu kendi çalışma alanıyla sınırlı.
- Erişim kontrolü: Google ile giriş veya özetlenmiş parolalar, güvenli oturum çerezleri, çalışma alanlarında roller ve yalnızca yetkili kişilerle sınırlı, salt okunur ve kayda geçen personel erişimi.
- Riskli adımlar için onay, reklam bütçelerinde kesin üst sınır ve bütün otomasyon için acil durdurma.
- Görevlerin, araç çağrılarının, iş devirlerinin, onayların ve personel erişiminin denetim kaydı.
- İstek sınırları ve kötüye kullanıma karşı koruma.
- 14, 60 ve 400 gün saklanan, geri yüklemesi test edilen şifreli gece yedekleri.
- Uygun güvenlik taahhütleri olan alt işleyenlerin seçilmesi ve her birine yalnızca görevinin gerektirdiği verinin verilmesi.

14. Ek 3: Alt işleyenler

Alt işleyenlerin güncel listesi, her birinin görevi ve konumuyla birlikte Güvenlik ve KVKK sayfamızdadır.