

NEXT4BIZ

KİŞİSEL VERİLERİN İŞLENME KOŞULLARINA İLİŞKİN SÖZLEŞME

MADDE 1. TARAFLAR

İşbu Kişisel Verilerin İşlenme Koşullarına İlişkin Sözleşme (bundan böyle kısaca "Sözleşme" olarak anılacaktır) Sahrayı Cedit Mahallesi Halk Sokak No: 40/4 34734 Kadıköy, İSTANBUL adresinde bulunan Next4biz Bilgi Teknolojileri A.Ş. ("Next4biz") ile

..... adresinde bulunan

.....

("Müşteri") arasında akdedilmiştir. İşbu Sözleşme kapsamında her biri ayrı ayrı "Taraflar" ve birlikte "Taraflar" olarak anılacaktır.

MADDE 2. AMAÇ VE KAPSAM

İşbu Sözleşme, yukarıdaki Taraflar arasında imzalanmış olan Next4biz Yazılım Lisans (SaaS) Sözleşmesi'nin (Bundan böyle kısaca "Anasözleşme" olarak anılacaktır) eki ve ayrılmaz parçası olup, Anasözleşme ile Next4biz'in Müşteri'ye sunacağı ürün ve hizmetler kapsamında Müşteri'nin Veri Sorumlusu olduğu kişisel verilerin işlenmesi faaliyetinin 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve ikincil mevzuatındaki yükümlülöklere uygun şekilde yerine getirilmesi amacıyla uyulacak kuralları belirlemektedir.

MADDE 3. TANIMLAR

İşbu Sözleşme'de aşağıdaki terimler için yanlarında bulunan tanımlar geçerli olacaktır:

Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Kişisel verilerin işlenmesi: kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan

yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

Kişisel Veri İhlali: Aktarılan, depolanan veya sair surette işlenen kişisel verilerin kazaen ve yetkisiz veya hukuka aykırı olarak yok edilmesine, kaybına, değiştirilmesine, yetkisiz şekilde ifşa edilmesine ya da bu verilere erişilmesine neden olabilecek, kişisel verilerin güvenliğini tehdit eden olayları,

Açık rıza: Kişisel verinin işlenmesine ilişkin ve amaç, sebep gibi Kanunda belirlenmiş konularda bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

Kişisel Verilerin İmhası: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

Kanun: 6698 Sayılı Kişisel Verilerin Korunması Kanununu,

Kurul: Kanun ile kurulmuş olan Kişisel Verileri Koruma Kurulunu,

Kurum: Kanun ile kurulmuş olan Kişisel Verileri Koruma Kurumunu,

Özel Nitelikli Kişisel Veri: Kişinin ırk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek, vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri, biyometrik ve genetik verileri,

Veri işleyen: veri sorumlusu adına ve onun verdiği yetkiye dayanarak kişisel verileri işleyen gerçek veya tüzel kişiyi,

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi, ifade eder.

MADDE 4. VERİ İŞLEME FAALİYETLERİ SIRASINDA UYULACAK KURALLAR

Veri İşleyen, işbu sözleşme uyarınca Veri Sorumlusu adına Kişisel Veri işlediği hallerde aşağıdaki yükümlülöklere uygun davranacaktır.

a. Veri İşleyen yalnızca Sözleşme'nin amacı ve hizmet kapsamında veya Veri Sorumlusu'nun talimatları doğrultusunda, Sözleşme'ye uygun bir biçimde Veri Sorumlusu adına Kişisel Verileri işleyecektir.

b. Veri İşleyen, Kişisel Verilerin hukuka aykırı olarak işlenmesini, bunlara hukuka aykırı olarak erişilmesini önlemeye, bunların muhafazasını sağlamaya, veri kaybı oluşmasını, verilerin yok olmasını, zarar görmesini, değiştirilmesini veya açıklanmasını engellemeye yönelik gerekli, (ilgili verilerin nitelikleri dikkate alınarak) teknik ve idari önlemleri alacaktır.

c. Veri İşleyen, veri işleme faaliyetini "gerekli olduğu ölçüde" prensibine uygun şekilde gerçekleştirecektir.

d. Veri Sorumlusu'nun sadece yurt içerisinde hizmet ve faaliyetlerini yürütüyor olması halinde, Veri İşleyen, Kişisel Verileri, Türkiye Cumhuriyeti sınırları dahilinde işleyecektir.

e. Hizmetin ifasına esas teşkil eden hukuki ilişkinin (sözleşmenin) sona ermesi halinde Veri İşleyen, Kanunen saklanması gerekenler hariç olmak üzere, kişisel verileri, Veri Saklama ve İmha Politikası uyarınca derhal veya en geç bir sonraki veri imha periyodunda imha eder.

f. Veri İşleyen, işlediği kişisel verileri sözleşmenin sona ermesi halinde 1 aylık süre içerisinde imha eder.

g. Veri İşleyen'e, işleme faaliyeti için aktarılan kişisel verilerin toplamı halinde İlgili Kişi'leri (Veri sahiplerini); KVKK kapsamında sahip olduğu haklar ve Kişisel Verilerinin işlenmesi koşulları bakımından aydınlatma yükümlülüğü ve veri toplamının hukuki dayanağını (Sözleşme veya açık rıza) yerine getirme yükümlülüğü Veri Sorumlusu'na aittir.

h. Veri İşleyen, İlgili Kişilerden, kişisel verilerinin düzeltilmesi, silinmesi, anonimleştirilmesi veya yok edilmesi ile ilgili bir talebin doğrudan kendisine iletilmesi halinde Veri Sorumlusu'nu ilgili talep hakkında haberdar eder. Veri Sorumlusu tarafından verilecek karara göre gereği yerine getirilir.

i. Özel Nitelikli Kişisel Veriler, Anasözleşme ve işbu Sözleşme kapsamında işlenecek kişisel veriler kapsamına girmemektedir. Next4biz SaaS platformu özel nitelikli kişisel verilerin işlenmesi amacıyla tasarlanmış bir ürün olmadığından Veri Sorumlusu, Veri

İşleyen'e, Özel Nitelikli Kişisel Veri aktarmamalıdır. (Bkz.

<https://www.next4biz.com/tr/legal/Legal-Security-Policies-Important-Notices-on-the-Management-of-Personal-data-TR.html>)

MADDE 5. VERİ İŞLEYEN'İN ÇALIŞANLARI VE YARDIMCILARI

Veri İşleyen, veri işleme faaliyeti sırasında çalışanlarının ve varsa alt-işleyenlerin sadece Anasözleşme'den kaynaklı hizmetlerin ifası kapsamında kişisel veri işlemesi gereken kişiler olduğunu, işbu Sözleşme kapsamındaki kişisel verilere ve işleme faaliyetlerine ilişkin gizlilik ve güvenlik taahhüdü veya uygun bir kanuni gizlilik ve güvenlik yükümlülüğü altında olmalarını sağlamakla yükümlüdür.

MADDE 6. KİŞİSEL VERİLERİN AKTARIMI

Veri İşleyen Ana Sözleşme'nin açıkça izin verdiği haller haricinde ve hizmet gerekleri haricinde (Veri İşleyen'in Türkiye'de yerleşik ver merkezlerinde kiraladığı sunucularına yapılan veri aktarımları hizmetin ifası gereğidir), Veri Sorumlusu'nun yazılı izni olmadıkça veya Türkiye Cumhuriyeti mevzuatı uyarınca yetkili idari veya adli makamlarınca hukuka uygun biçimde talep edilmedikçe Kişisel Veriler'i 3. Kişilere aktarmayacaktır. Yetkili idari veya adli makamların hukuka uygun talepleri karşısında veri paylaşılması gereken hallerde, Veri İşleyen Veri Sorumlusu'nu derhal durumdan haberdar edecek ve Taraflar'ın hukuki ve ticari menfaatleri açısından gerekli iş birliğinde bulunacaktır.

MADDE 7. TEKNİK VE İDARİ TEDBİRLER

7.1. Veri Sorumlusu ve Veri İşleyen işbu Sözleşme kapsamında veri işleme faaliyetleri sırasında aşağıdaki tedbirleri alacaktır:

- a. Kişisel verilerin muhafazasına ilişkin fiziksel güvenlik önlemleri alınmış olması,
- b. Çalışanların kişisel veri güvenliği konusunda eğitilmesi ve farkındalıklarının artırılması konusunda periyodik bilgilendirme yapılması,
- c. Yetki matrisinin oluşturulmuş ve işletiliyor olması,
- d. Yetki kontrol sürecinin tanımlanması ve kontrollerinin periyodik olarak yapılması,
- e. Ağ güvenliğinin sağlanmasına yönelik süreçlerin kurgulanmış olması,

f. Uygulama güvenliğine yönelik önlemlerin alınmış olması, periyodik sızma testlerinin işletilmesi,

g. Şifre yönetim süreçlerinin tanımlanmış olması ve işletilmesi,

h. Saldırı tespit ve önleme sistemi kurgulanmış olması,

i. Olası yetkisiz erişim tehditlerine karşı güvenlik duvarı kullanılması.

j. Erişim loglarının yönetimine yönelik sürecin tanımlanması ve işletilmesi,

k. Veri ihlali durumunda uygulanacak bildirim süreçlerine ilişkin prosedürün tanımlanması ve uygulanması,

7.2. Veri Sorumlusu tarafından Next4biz ürünü uyarlanırken ve kullanılırken kişisel verilerin yönetimi konusunda aşağıdaki hususlara dikkat edilecektir;

a. Next4biz uygulaması ile ilgili teknik destek alınan yardım masasına ve destek e-posta adreslerine, kişisel veriler gönderilmemelidir.

b. Müşteri ile iletişime geçilen her bir kanalda "Bilgilendirme/Aydınlatma Metni"ne yer verilmelidir.

c. Müşterilere tanıtım/pazarlama amaçlı kampanya e-posta veya sms'i gönderilecek ise izin alınmalıdır.

d. IYS (İzinli İletişim Yönetim Sistemi) ile entegrasyon sağlanarak izin ve red bilgileri güncel tutulmalıdır.

e. Müşterilere gönderilen izinli e-posta ve sms kampanya iletilerinde, yeni bir ileti alınmamasına yönelik izin kaldırma linki yer almalıdır.

f. Görev tanımlarına uygun yetkilendirme ve rol yapısını tarifleyen yetki matrisi hazırlanmalıdır. Yetki matrisi kapsamında kişisel veri içeren alanlara ilgili kullanıcıların sadece görev ve sorumluluğu ile sınırlı olacak şekilde yetkilendirilmesi sağlanmalıdır.

g. Next4biz uygulamasında toplanan/girişi yapılan veriler; veriyi görme ve işleme yetkisi olmayan birimlerle ve üçüncü partilerle paylaşılmamalıdır.

h. Next4biz uygulamasında tutulan kişisel verilerin amacı dışında kullanılmasını engellemek adına; uygulama kullanıcılarına bu konuyu hatırlatacak bilgilendirmeler

hazırlanmalı, düzenli olarak paylaşılmalıdır.

i. Next4biz arayüzünde oluşturulacak özel veri alanları "ölçülülük" ve "veri minimizasyonu" ilkelerine sadık kalınarak tanımlanmalıdır.

j. Next4biz uygulaması ile özel nitelikli kişisel veriler toplanmamalı ve işlenmemelidir.

k. Müşterilerin her türlü finansal verisinin ve ödeme araçlarına ilişkin hassas verilerinin Next4Biz uygulamasına yüklenmemesi için gerekli uyarılar arayüzde tanımlanmalıdır.

l. E-posta ve sms ile gönderilen otomatik veya manuel bilgilendirme ileti şablonlarında ve iletilerde müşteriye ait gerekli olmayan kişisel veriler yer almamalıdır.

m. Bilgilendirme e-postalarının sonuna "KVKK aydınlatma metni" ve e-postanın gönderim amacını ifade eden bilgilendirme eklenmelidir.

MADDE 8. BİLGİ GÜVENLİĞİ TEST ve KONTROLLERİ

a. Veri İşleyen, Next4biz SaaS platformu için düzenli olarak gerçekleştirdiği sızma (penetration) testlerinin yönetici özet raporlarını talep etmesi halinde Veri Sorumlusu ile paylaşacaktır.

b. Veri Sorumlusu veya yetkilendirdiği kişiler tarafından, Veri İşleyen'den önceden izin alınmaksızın, penetrasyon, sızma, IDOR vb kategorilerde regülatif veya esnek güvenlik testleri, NIST, MITRE, OWASP vb çerçeve ve vektörlerde atak deneme ve gözden geçirmeleri, performans testleri yapılması, saldırı düzenlenmesi, zararlı istek gönderilmesi yasaktır.

MADDE 9. VERİ GÜVENLİĞİ İHLALİ HALİNE İHBAR YÜKÜMLÜLÜĞÜ

Veri İşleyen, Veri Sorumlusu adına işlediği kişisel veriler veya bu verilerin bulunduğu ortamlarda bir Veri İhlali veya Veri İhlali olarak nitelendirilebilecek bir vaka gerçekleşmesi halinde, ihlalin gerçekleştiğini öğrendiği tarihten itibaren en geç 48 (Kırk Sekiz) saat içinde Veri Sorumlusu'na bildirecektir.

MADDE 10. SORUMLULUK

Veri İşleyen tarafından Anasözleşme ve işbu Sözleşme kapsamında işlenen kişisel verilerin Kanuna ve ilgili mevzuata aykırı şekilde işlenmesi veya Veri İşleyen tarafından işbu Sözleşme'deki yükümlülüklerinin kusurlu şekilde ihlali halinde, Veri Sorumlusu'nun karşı karşıya kalabileceği ilgili maddi zararlar sebebiyle Veri İşleyen sorumlu olduğunu beyan, kabul ve taahhüt eder. Veri İşleyen'in bu sorumluluğu Taraflar arasındaki Anasözleşme'de belirlenen sorumluluk üst limiti ile sınırlıdır.

MADDE 11. SÖZLEŞMENİN YÜRÜRLÜĞÜ

İşbu Sözleşme, Taraflarca imzalandığı tarihte yürürlüğe girer. Taraflar arasında imzalanmış olan Anasözleşme'nin eki ve ayrılmaz parçası olup, yorumlanmasına Anasözleşme içindeki hükümlere göre hizmet esasları dikkate alınır.

Anasözleşme'nin feshi halinde işbu Sözleşme kişisel verilerin Veri İşleyen tarafından imhası ile birlikte yürürlükten kalkar.

Tarih:	
Next4biz Bilgi Teknolojileri A.Ş.	