

GDPR Uyumluluđu

Next4biz'in Genel Veri Koruma Yönetmeliđi (GDPR) ile ilgili Gizlilik Politikası.

Next4biz

Genel Veri Koruma Yönetmeliđi (GDPR) Gizlilik Politikası

Kurul/Yönetim tarafından onaylanma: Bilgi Güvenliđi, GDPR ve Teknoloji Komitesi.

Politika 18.05.2018 tarihinde yürürlüđe girdi.

Kapsam :

GDPR Komitesi bu politikadan sorumludur. Next4biz, belirli kişisel verileri toplamakta ve işlemektedir. Bunlar; müşteriler, tedarikçiler, iş bağlantıları, çalışanlar ve kuruluşun bir ilişkisi olduđu veya iletişim kurması gerekebilecek diđer kişileri içerebilir. Bu politika, bu kişisel verilerin şirketin veri koruma standartlarını karşılamak ve yasalara uymak için nasıl toplanması, kullanılması ve saklanması gerektiđini açıklar. Bu politika tüm personel için geçerlidir. Bu politika, internet ve e-posta kullanımı ile ilgili diđer politikalarımızı desteklemektedir.

Bu politika, kişisel verileri nasıl korumaya çalıştığımızı ve personelin, çalışmaları sırasında erişebilecekleri kişisel veri kullanımını yöneten kuralları anlamalarını sağladığımızı belirler. AB Genel Veri Koruma Yönetmeliđi (GDPR) kişisel verilerin etik olarak ele alınmasını tanımlar.

Yasal Gereksinimler:

Veri işlememiz için uygun bir yasal dayanak (veya temel) belirlenmiştir. Kişisel verilerle yasa dışı hiçbir işlem yapılmamaktadır.

Meşruiyet / Yasalara Uygunluk:

Ver işlemenin ilgili kişileri nasıl etkileyebileceğini ve olumsuz etkileri değerlendirilmiştir. Kişisel veriler, yalnızca iş gereksinimleri doğrultusunda toplanmakta ve işlenmektedir. Kişisel verilerini toplama konusunda gerekli bilgilendirmeler yapılmaktadır.

KVKK Aydınlatma metni aşağıdaki linktedir;

[KVKK Aydınlatma Metni](#)

Şeffaflık:

Bilgi edinme hakkının şeffaflık yükümlülüklerine uyuyoruz. Veri işleme amaçlarımızı açıkça belirledik. Bireyler için gizlilik bilgilerimize veri işleme amaçlarımızın detaylarını ekliyoruz. İşlemlerimizi düzenli olarak inceliyor ve gerektiğinde belgelerimizi ve bireyler için gizlilik bilgilerini güncelliyoruz. Kişisel verileri, yasada belirtilen yasal bir yükümlülük veya işlev dışında yeni bir amaç için kullanmayı planlıyorsak, bunun orijinal amacımızla uyumlu olup olmadığını veya yeni amaç için özel onay aldığımızı kontrol ediyoruz.

Veri Minimizasyonu :

Yalnızca belirtilen amaçlarımız için ihtiyacımız olan kişisel verileri toplar ve bu amaç doğrultusunda yeterli olacak desen ve detayda bilgileri işleriz. İşlediğimiz ve sakladığımız kişisel verileri periyodik olarak gözden geçirir ve talep doğrultusunda ve/veya iş gereksinimleri sonunda anonimleştirir veya imha ederiz.

Özel Nitelikli Kişisel Veriler: Bir bireyin ırksal veya etnik kökenleri, siyasi görüşleri, dini veya benzer inançları, sendika üyeliği (veya üyeliği olmayan), fiziksel veya zihinsel sağlık veya durum, cezai suçlar veya ilgili davalar hakkında kişisel verileri işlemeyiz; kişisel verileriniz bu politikaya göre sıkı bir şekilde kontrol edilmektedir.

Veri Koruma Yasası: Veri Koruma Yasası, Next4biz dahil olmak üzere kuruluşların kişisel bilgileri nasıl toplaması, kullanması ve saklaması gerektiğini açıklamaktadır. Bu kurallar, verilerin elektronik olarak, kağıt üzerinde veya diğer malzemeler üzerinde depolanmasına bakılmaksızın uygulanır. Yasalara uymak için meşru şekilde bilgilerin toplanmasına, kullanılmasına, işlenmesine ve güvenli bir şekilde saklanarak ve yasalara aykırı olarak ifşa edilmemesine özen gösterilir.

Veri Koruma Yasası sekiz önemli ilke ile desteklenmektedir. Bu ilkeler ışığında kişisel veriler tarafımızdan; ;

1. Adil ve yasalara uygun olarak işlenir
2. Sadece belirli, yasal amaçlar için alınır.
3. Yeterli ve ilgili olmasına dikkat edilir.
4. Doğru ve güncel olmasına dikkat edilir.
5. Gerekenden daha uzun süre tutulmaz.
6. Veri sahiplerinin haklarına uygun olarak işlenir.
7. Gerekli güvenlik tedbirleriyle korunur.

Veri kontrolü :

Komite, sahip olduğu yetkinlikle, belirtilen ilkelere uygunluğu periyodik şekilde gözden geçirir. Veri işleyen statüsünde olan tedarikçilerle yapılan sözleşmelerin GDPR'ye uygun olmasını sağlar.

Doğruluk ve İlişki Düzeyi:

İşlenen kişisel verinin işleme amacıyla uygunluğu ve işlenecek verinin gereksinim kadar olması sağlanır. Tek bir amaç için elde edilen kişisel verileri herhangi bir bağlantılı amaç için işlemiyoruz.

Veri Güvenliği :

Kişisel verilerinizi kaybolmaya veya yanlış kullanıma karşı güvende tutarız.

- Verilerin basılı kağıda depolanması durumunda, Temiz Masa Politikamıza göre yetkisiz personelin erişemeyeceği güvenli bir yerde saklanmaktadır.
- Basılı veriler ISO 27001 kılavuzlarımıza göre gerekli olmadığında imha edilmektedir.
- Bilgisayarda depolanan veriler, (Şifre Politikası) uyarınca düzenli olarak değiştirilen güçlü şifrelerle korunmaktadır.
- USB Politikamıza uygun olarak bellek çubuklarında veri saklanmamaktadır.
- Kişisel veriler içeren sunucular ulusal ve güvenli bir veri merkezinde saklanır
- Veriler, şirketin yedekleme prosedürleri doğrultusunda düzenli olarak yedeklenir.

Ticari Amaçlar

İşlediğimiz kişisel veriler, ticari amaçlarımız doğrultusunda kullanabileceğimiz kapsamdadır.

Personel, idari, mali, düzenleyici, bordro ve iş geliştirme amaçları aşağıdaki ticari başlıkları içerir:

- Yasal, düzenleyici ve kurumsal yönetim yükümlülüklerimize ve uygulamalarımıza uygunluk – Düzenleyici kurumlar tarafından yapılan soruşturmaların bir parçası olarak veya yasal işlem veya taleplerle bağlantılı olarak bilgi toplama – İş politikalarına uyulmasını sağlamak (e-posta ve internet kullanımını kapsayan politikalar gibi)
- İşlemlerin kaydedilmesi, eğitim ve kalite kontrol, ticari açıdan hassas bilgilerin gizliliğinin sağlanması, güvenlik denetimi, kredi puanlama ve kontrol gibi operasyonel nedenler – Şikayetlerin araştırılması – Referansların kontrol edilmesi, güvenli çalışma uygulamalarının sağlanması, personelin sistemlere ve tesislere erişiminin izlenmesi ve yönetilmesi ve personel devamsızlığı, yönetim ve değerlendirmeler – Personel davranışının izlenmesi, disiplin kurallarına uygunluğun sağlanması
- Pazarlama- hizmetlerin iyileştirilmesi, yazılımsal iyileştirme ve düzeltmelerin yapılması
- Kişisel veriler İş başvurusunda bulunanlar, mevcut ve eski çalışanlar, ajans, sözleşme ve diğer personel, müşteriler, tedarikçiler ve pazarlama kişileri gibi tanımlanabilir bireylerle ilgili bilgiler. Topladığımız kişisel veriler şunları içerebilir: bireylerin iletişim bilgileri, eğitim durumu, finansal ve ödeme bilgileri, sertifika ve diplomaların ayrıntıları, eğitim ve beceriler, medeni durum, uyruk, iş unvanı ve CV.

Veri Saklama :

Kişisel veriler amacı dışında ve iş amaçları gereğinden daha uzun süreli saklanmamakta ve işlenmemektedir. Gerekli olan veri saklama süresi, kişisel verilerin elde edilmesinin nedenleri göz önünde bulundurularak, her bir vakanın koşullarına bağlı olarak, veri saklama politikamız ile uyumlu bir şekilde belirlenmektedir. Detaylar için [Veri Saklama ve İmha Politikamıza](#) bakabilirsiniz.

Uluslararası Veri Aktarımı:

Şirketimizin sunduğu hizmetlerin gerektirdiği hallerde ve zorunlu olan ölçüde üçüncü parti iş ortaklarımızın veri merkezlerinde, güvenli ortamlarda verilerin saklanması amacıyla kişisel veriler **yurt içinde** işlenir.

Operasyonel süreçlerin yürütülmesi kapsamında kişisel veriler Türkiye dışında hiçbir ülkeye aktarılmamaktadır.

Diğer aktarımlar ise, Komite onayı ile gerçekleşmektedir.

Veri Koruma Riskleri:

Politikada yer alan prensip ve roller Next4biz'in aşağıda yer alan riskler de dahil olmak üzere, veri güvenliği risklerinden korunmasına yardımcı olur:

- Gizlilik ihlali.
- Veri işleme süreçlerinin tanımlı olmaması.

Sorumluluklar:

- Next4biz veya Next4biz ile birlikte çalışan kişi ve kurumların verilerin toplanmasını, saklanmasını ve uygun şekilde ele alınmasını sağlama sorumluluğu vardır. Kişisel verileri işleyen her ekip, bu politika ve veri koruma ilkeleri doğrultusunda ele alınmasını ve işlenmesini sağlamaktadır.
- Bilgi Güvenliği, GDPR ve Teknoloji Komitesi nihai olarak Next4biz'in yasal yükümlülüklerini yerine getirmesinden sorumludur.

Bilgi Güvenliği, GDPR ve Teknoloji Komitesi veri koruma görevlisi rolüne sahiptir. Hizmet alınan bulut veri merkezi sorumlulukları ile pazarlama faaliyetini yürütecek roller ve sorumluluklar, Komite tarafından atanmakta ve gözden geçirilmektedir. Komite aşağıdaki maddelerden sorumludur:

- Veri koruma sorumlulukları, riskleri ve sorunları hakkında şirket yönetimini güncel tutmak.
- Tüm veri koruma prosedürlerinin ve ilgili politikaların üzerinde mutabık kalınan bir programa göre gözden geçirmek.
- Bu politikanın kapsamına giren kişiler için veri koruma eğitimi ve bilgilendirmeleri düzenlemek.

- Personelden ve bu politikanın kapsadığı diğer herkesten gelen veri koruma sorularını ele almak.
- Next4biz'in bu veriler hakkında tuttuğu verileri görmek için bireylerden gelen taleplerle ilgilenmek ('konu erişim istekleri' olarak da adlandırılır).
- Şirketin verilerini işleyebilecek üçüncü taraflarla yapılan sözleşmeleri veya sözleşmeleri kontrol etmek ve onaylamak.

Hizmet Alınan Bulut Veri Merkezi Sorumlulukları:

- Veri depolamak için kullanılan tüm sistem, hizmet ve ekipmanların kabul edilebilir güvenlik standartlarını karşıladığından emin olmak.
- Güvenlik donanımı ve yazılımının düzgün çalıştığından emin olmak için düzenli kontroller ve taramalar yapmak.
- Şirketin verilerini depolamak veya işlemek için kullanmayı düşündüğü üçüncü taraf hizmetlerini değerlendirmek.

Pazarlama Yöneticisinin Sorumlulukları:

- E-posta ve mektup gibi iletişimlere iliştirilmiş veri koruma bildirimlerini onaylamak.
- Gazetecilerden veya gazete gibi medya kuruluşlarından gelen veri koruma sorgularının ele almak.
- Gerekliğinde, pazarlama girişimlerinin veri koruma ilkelerine uymasını sağlamak için diğer personel ile birlikte çalışmak.

Genel Personel Yönergeleri:

Bu politikanın kapsadığı verilere erişebilen kişi veya kişiler sadece çalışmaları için gerekmesi halinde ve gerektiği kadarıyla verilere erişebilmektedirler. Gizli bilgilere erişim gerektiğinde, çalışanlar bu bilgileri bölüm yöneticilerinden talep edebilir. Next4biz, tüm çalışanlara veri işlerken sorumluluklarını anlamalarına yardımcı olacak bilgilendirmeleri sağlar. Çalışanlar, etkin önlemler alarak ve aşağıdaki yönergeleri izleyerek tüm verileri güvende tutarlar. Özellikle, güçlü şifreler kullanır ve kesinlikle paylaşmazlar. Kişisel veriler şirket içinde veya dışında yetkisiz kişilere açıklanmaz.

Veri Kullanımı :

- Kişisel verilerle çalışırken, çalışanlar gözetimsiz bırakıldığında bilgisayarlarının ekranlarının her zaman kilitli olduğundan emin olunur.
- Kişisel veriler gayri resmi olarak paylaşılmaz. Özellikle, bu iletişim şekli güvenli olmadığından gerekli tedbirler alınmadan (şifreleme) ve iş gereksinimleri doğrultusunda zorunlu olmadıkça e-posta ile gönderilmez.
- Çalışanlar kişisel verilerin kopyalarını kendi bilgisayarlarına kaydetmemeye özen gösterirler.

Veri Depolama:

Bu kurallar, verilerin nasıl ve nerede güvenli bir şekilde saklanması gerektiğini tanımlar. Verilerin güvenli bir şekilde saklanmasıyla ilgili sorular BT yöneticisine veya veri denetleyicisine yönlendirilebilir. Veriler kağıda depolandığında, yetkisiz kişilerin göremediği güvenli bir yerde saklanır. Bu yönergeler genellikle elektronik olarak depolanan ancak bir nedenle yazdırılan veriler için de geçerlidir. Gerektiğinde kağıt veya dosyalar kilitli bir çekmecede veya dosya dolabında tutulur. Çalışanlar, yazıcıda olduğu gibi, yetkisiz kişilerin görebileceği yerlerde kağıt ve çıktıların kalmadığından emin olur. Veri çıktıları, artık gerekli olmadığından güvenli bir şekilde imha edilir. Veriler elektronik olarak depolandığında, yetkisiz erişim, yanlışlıkla silinme ve kötü niyetli saldırı girişimlerine karşı korunur. Veriler, düzenli olarak değiştirilen ve çalışanlar arasında paylaşılmayan güçlü parolalarla korunur. Veriler yalnızca belirlenmiş sürücüler ve sunucularda depolanır ve yalnızca onaylı bir bulut bilişim hizmetlerine yüklenir. Kişisel veriler içeren sunucular, genel ofis alanından uzakta, güvenli bir yerde bulunur. Veriler gerekli olan periyotlarda yedeklenir. Bu yedeklemeler, şirketin standart yedekleme prosedürleri doğrultusunda düzenli olarak test edilir. Veri içeren tüm sunucular ve bilgisayarlar onaylı güvenlik yazılımı ve güvenlik duvarı ile korunur.

Konu Erişim İstekleri

Next4biz tarafından tutulan kişisel verilere konu olan tüm bireyler:

- Kendileri hakkında hangi bilgilerin tutulduğunu ve nedenini sorabilir.
- Bu verilere erişim sağlama yöntemlerini sorabilir.
- Nasıl güncel tutulacağı konusunda bilgi sahibi olabilir.

- Next4biz'in veri koruma yükümlölüklerini nasıl yerine getirdiğinden haberdar olabilir.

Bir kiři yukarıdaki bilgilere erişmek amacıyla Next4biz ile temasa geçerse buna konu erişim isteğı denir. Kiřilerin konuya yönelik erişim istekleri, Next4biz'e ait [kayıtlı e-posta adresi] e-posta adresine gönderilen mesaj ile yapılır. Next4biz i30 gün içinde cevap verir. Next4biz herhangi bir bilgiyi teslim etmeden önce konu erişim isteğı yapan kiřinin kimliğini her zaman doğrular. Bazı durumlarda, Veri Koruma Yasası, kişisel verilerin veri sahibinin rızası olmadan kolluk kuvvetlerine ifřa edilmesine izin verir. Yasal tüm kořulların varlığı halinde Next4biz Formalis istenen verileri açıklar.

Bilgi Verme/Edinim :

Next4biz, bireylerin verilerinin işlendiğini ve anladıklarını bilmelerini sağlamayı amaçlamaktadır. Bu doğrultuda;

- Verilerin nasıl kullanıldığı,
- Haklarını kullanma konularında,
- Aydınlatma yükümlölüğünü yerine getirir

Next4biz'in bireylerle ilgili verilerin nasıl kullanıldığını belirten gizlilik politikası aşağıda yer almaktadır.

[Gizlilik Politikası](#)