

Kurumsal Müşterilerimizin Next4biz uygulaması üzerinde müşteri ve her türlü kişisel bilgilerini yönetirken, süreç tasarımı, yetkilendirme ve konfigürasyon yaparken veya uygulamayı kullanırken KVKK, müşteri sırrı ve hassas veri kapsamındaki kanun ve yönetmeliklere uyum ve veri güvenliği açısından aşağıdaki konulara dikkat etmesi önerilmektedir;

1. Kişisel verinin işlenmesine yönelik, Müşteri ile iletişime geçilen her bir kanalda “Bilgilendirme/Aydınlatma Metni”ne yer verilmelidir.

İnternet ortamı üzerinden gerek iletişim, gerek veri giriş formları ile müşteri bilgileri veya bildirim toplanırken kurumsal KVKK Aydınlatma/Bilgilendirme metninin erişim linki ilgili form üzerinde yer almalı ve işlenecek verinin amacına uygun onay alınarak, toplanan verinin ne amaçla kullanılacağı ifade edilmelidir.

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

Müşterilere e-posta veya sms yolu ile tanıtım/pazarlama veya kampanya/reklam amaçlı içerik gönderimi yapılacak ise ilgili iletişim kanalı için iletişim izni alınmalıdır. İletişim izinleri bir veritabanında tarihçe ile kayıt altına alınmalı ve güncel tutulmalıdır. Hangi amaçla izin alınmış ise o amaç dışında gönderim yapılmamalıdır.

Next4biz CRM üzerinden e-posta ve sms gönderimi yaparken güncel izin bilgileri ile gönderim yapılmalıdır. Bu amaçla;

İletişim izni bilgisi Next4biz CRM’e aktarılmalı ve bu ortamda da güncel tutulmalıdır. Next4biz CRM tarafından güncel izin bilgileri kurum tarafından sağlanacak web servisler aracılığı ile toplu olarak sorgulanabilir olmalıdır. IYS olarak adlandırılan izin sistemi ile entegrasyon bu süreçte uyulması gereken mevzuat gereksinimidir.

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

Müşterilerden alınan izin bilgileri IYS sistemine aktarılmalıdır. Müşteriler tarafından IYS üzerinden yapılan izin/red tercihleri alınmalı ve Next4biz CRM'e aktarılmalıdır. Bu amaçla;

İzinli İletişim Yönetimini sağlayan IYS Entegratörü firmalar ile çalışılabilir. Entegratör firma, kurum adına iletişim izni alma, izin kaldırma, İYS'ye aktarma, İYS'den gelen verilere göre izinli iletişim bilgilerini güncelleme işlevlerini sağlar.

IYS Entegratör firma tercih ederken aşağıdaki entegrasyonları sağladığı teyit edilmelidir;

- *İzin bilgilerini yazabilmek için entegrasyon web servisi (API) sağlamalıdır.*
- *Güncellenen izin bilgilerini Next4biz CRM'e yazabilmelidir.*
- *İzin bilgilerinin toplu olarak sorgulanabilmesi için web servisi (API) sağlamalıdır.*

Next4biz'in hazır entegrasyonu bulunan entegratör firmalar tercih edilebilir.

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

Müşterilere gönderilen e-posta ve sms kampanyalarında, gönderim listelerinden çıkabilmeleri için linkler yer almalıdır. Müşteriler ileti almak istememesi halinde bu linklere tıklayarak iletişim iznini kaldırabilirler.

5. 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.

Müşteri ve her türlü kişisel bilgilerini arama ve erişim yetkilendirmeleri ile birlikte, bildirimlerde arama, bildirim veya müşteri özelinde tanımlanan veri alanlarına erişim için kişisel verinin, veri sınıflandırma kategorisi kapsamında kurumunuzca belirlenen kritiklik seviyesine göre rol/yetki matrisi hazırlanmalıdır. Bu matris düzenli gözden geçirilmeli ve güncel tutulmalı, görev değişiklikleri ve işten ayrılma gibi durumlar işlemin gerçekleşmesi sürecinde tamamlanmalıdır.

Next4biz üzerindeki tanımlamalar bu matrise göre yapılmalı ve canlıya kullanım öncesinde ve sonrasında periyodik olarak kontrol edilmelidir. Yetkilendirmeler,

“sadece gerektiği kadar ve gereken kişilere olmalı” prensibine uygun şekilde gerçekleştirilmelidir.

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

Otomatik iş akışları ve manuel yönlendirmeler ile bildirimlerin hangi iş birimlerine veya iş ortaklarına yönlendirilebileceği belirlenmelidir. Veri alanları ve kullanıcı bazında yetkilendirmeler görevler ayrılığı ve yetki grupları matrisi kapsamında ve iş ihtiyacı çerçevesinde gerçekleştirilmelidir. Amacı dışında yönlendirme veya akış tanımlanmamalıdır. E-posta vb... yöntemler ile bu veriler uygulama dışı ortamlara taşınmamalıdır.

7. Next4biz uygulamasında tutulan kişisel verilerin amacı dışında kullanılmasını engellemek adına; uygulama kullanıcılarına bu konuyu hatırlatacak bilgilendirmeler hazırlanmalı, düzenli olarak paylaşılmalıdır.

Ayrıca kurumunuz içerisinde ve tedarikçilerinize bilgilendirmeler düzenli olarak yapılmalı ve gerekli sözleşmeler bu hükümleri de kapsayacak şekilde imzalanmalıdır.

Bilgilendirme metinleri kullanıcılar için duyuru ve bilgi birikimi olarak hazırlanarak, uygulama içerisinde paylaşılabilir.

Duyuru Metni Örneği: Uygulama üzerinde oluşturulan ve toplanan kişisel veriler ancak müşteri bilgilerinin yönetimi, taleplerinin karşılanması ve iş süreçlerinin işletimi amacı ile kullanılacaktır. Bunun dışında uygulama ortamı dışına çıkarılmamalı veya farklı amaçlar için kullanılmamalıdır.

8. Next4biz arayüzünde oluşturulacak özel veri alanları “ölçülülük” ve “veri minimizasyonu” ilkelerine sadık kalınarak tanımlanmalıdır.

Müşteri bilgilerinin yönetiminde, taleplerinin karşılanmasında ve iş süreçlerinin işletiminde gerekli olmayan veri alanlarının oluşturulmamasına dikkat edilmelidir.

KVKK iyi uygulama rehberine uygun şekilde tanımlama ve kontroller yapılmalıdır.

9. Next4biz uygulaması ile özel nitelikli kişisel veriler toplanamaz ve işlenemez.

6698 sy. Kanun kapsamında özel nitelikli kişisel veriler; ilgilinin, ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileridir.

- a. Next4biz uygulaması üzerinde özel nitelikli kişisel verinin girilebileceği veri alanları oluşturulmalıdır.
- b. Özel nitelikli kişisel verilerin kullanıcılarınız veya müşteriler tarafından Next4Biz uygulamasına yüklenmemesi için gerekli uyarılar arayüzde tanımlanmalıdır.

Bildirim formlarında etiket (label) türünden veri alanları oluşturularak ilgili açıklamalar eklenmelidir. Benzer şekilde dosya yükleme alanları için de bu bilgilendirme metinleri kullanılmalıdır.

Örnek metin: Lütfen bu alana sağlık, adli sicil, siyasi görüş vb özel nitelikli kişisel veri yazmayınız / yüklemeyiniz.

- c. Özel nitelikli kişisel veriye ilişkin kurumunuz, kullanıcılarınız ve tedarikçileriniz tarafından bilgi girişi yapılmamasına özen gösterilmeli, gerekli bilgilendirmeler periyodik olarak yapılmalıdır.
- d. Özel nitelikli kişisel veri içeren bir e-posta veya müşteri bildirim açıklaması alınması halinde bildirim içerisindeki özel nitelikli veri, ilgili kurum kullanıcılarınız tarafından ivedilikle silinmelidir.

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

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

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

Örnek Metin: Bu e-posta, firmamıza ilettiğiniz bildiriminize istinaden bilgilendirme amaçlı olarak size yönlendirilmiştir. Firmamıza ilettiğiniz bir bildiriminiz

bulunmuyorsa ve sizinle ilgili değilse, lütfen iletiş[(#)] (kurumsal mail adresiniz) mail adresine bildiriniz.

13. Teknik yardım masası, e-posta, vb... gibi kişisel verilerin yer alması gerekmeyen uygulama ve ortamlara, kişisel verileri içeren ekran görüntüsü, belge vb... yüklenmemelidir.

Next4biz uygulaması ile ilgili teknik destek alınan yardım masasına, destek taleplerinin çözümünde gerekli olmayan kişisel veriler girilmemeli ve yüklenmemelidir.

Yüklenen dosyalarda, sorunun çözüm süreci için gerekli olan bilgi dosyaları için, anonimleştirme ve şifreleme gibi güvenlik önlemlerinin alındığından emin olunmalıdır.

Bu konuda gerekli farkındalık bilgilendirmesini periyodik olarak kurum çalışanlarınıza ve tedarikçilerinize yapmalısınız.

14. Müşterilerinizden gelen kişisel veri anonimleştirme taleplerini Next4biz API ile veya Yardım Masası üzerinden ileterek karşılayabilirsiniz.

Kişisel verilerin anonimleştirilmesi için API üzerinden anonimleştirme metodunu kullanabilirsiniz. Alternatif olarak yardım masası üzerinden bildirim açarak Next4biz destek ekibine talebinizi iletebilirsiniz. Anonimleştirme talepleriniz içerisinde kişisel veri yer almamalı, bu verileri adresleyen veri deseni ve/veya veriyi adresleyen (teknik) bilgi bulunmalıdır.

Anonimleştirilen veriler tekrar geri döndürülemeyecektir. Bu nedenle operasyonel süreklilik ve yasal sorumluluklar açısından şikayet, süreç vb... kayıtlarda anonimleştirme kurumsal olarak değerlendirilmelidir.

15. Next4biz Yardım Masası Bilgi Birikiminde yer alan Bilgi Güvenliği Kategorisi altındaki yöntemler uygulanmalı ve periyodik olarak kontrol edilmelidir.

Next4biz Yardım Masası Knowledge Base: Bilgi Güvenliği Kategorisi

- *Şifre yönetimi nasıl yapılır?*
- *Yetkilendirme yönetimi nasıl yapılır?*
- *Müşteri verilerine erişimi etkileyen yetkiler nelerdir?*

- *Bildirimlerde kısıtlı arama yetkisi nasıl verilir?*
- *Müşteri arama fonksiyonu nasıl kısıtlanır?*
- *Kullanıcılar için IP kısıtlamasını nasıl kullanıma açabilirim?*
- *Yardım Masasını kullanırken dikkat edilecek hususlar nelerdir?*
- *Login İşlemlerinde İki Seviyeli Doğrulama*
- *Gizli Bildirim Yönetimi*
- *Müşteri Veri Alanlarının Yetkilendirmesi*
- *Müşteri Özel Alanı Yönetimi Nasıl Yapılır?*
- *Bildirim Özel Alanı Yönetimi Nasıl Yapılır?*

16. Dış Hizmet Alımı

Kişisel verilerin işlenmesi sürecinde bir alt yüklenici veya dış hizmet alımı söz konusu ise bu durumda mutlaka Next4Biz'e bilgi verilmeli, gerekli mutabakat sağlanarak, hukuki şartlar, sözleşmeler, teknik altyapı konusunda uygunluk ve onay alınarak ilerlenmelidir.