## 1. AMAÇ

Bu politika Credence Risk Yönetimi ve Danışmanlık A.Ş. (Şirket) tarafından gerçekleştirilen faaliyetlerde elde edilecek kişisel verilerin, Şirketin 6698 sayılı Kişisel Verilerin Korunması Kanununda (Kanun) tanımlanan veri sorumlusu ve veri işleyici sorumluluklarına göre, ham ve işlenmiş verinin saklanması ile saklama süresi sonunda kişisel verilerin imha edilmesi süreçlerini tanımlamak amacıyla oluşturulmuştur.

## 2. KAPSAM

Bu politika; Şirket sahiplerinden, çalışanlarından, çalışan adaylarından, ziyaretçilerinden, Şirketin iş ortaklarından, tedarikçilerinden, çözüm ortaklarından, müşterilerinden, potansiyel müşterilerinden, ilişkide bulunulan üçüncü kişilerden elde edilen veya bu kişi ya da kurumlarla paylaşılan kişisel verilerin saklanması ve imha edilmesi ilkelerini tanımlar.

## 3. TANIMLAR

| | | |
|---|---|---|
| **Şirket** | : | Credence Risk Yönetimi ve Danışmanlık A.Ş. |
| **Kanun** | : | 6698 sayılı Kişisel Verilerin Korunması Kanunu |
| **Kişisel Veri** | : | Belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgidir. |
| **Özel Nitelikli Kişisel Veri** | : | Kişilerin 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. |
| **Veri İşleme** | : | Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla ilk defa elde edilmesiyle başlayan ve devamındaki bütün işlemlerden oluşan süreçtir. |
| **İlgili Kişi** | : | Kişisel verisi işlenen “Gerçek” kişiyi ifade eder. |
| **Veri Sorumlusu** | : | Kişisel verilerin işleme amaçlarını ve yöntemlerini belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişidir. |
| **Veri İşleyen** | : | Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişidir |
| **Açık Rıza** | : | Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır |
| **KVK Kurulu** | : | Kişisel Verileri Koruma Kurulu. |
| **Alıcı Grubu:** | : | Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişilerdir. |
| **Doğrudan Tanımlayıcılar** | : | Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılardır. |
| **Dolaylı Tanımlayıcılar** | : | Diğer tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcılardır. |

| | | |
|---|---|---|
| **İlgili kullanıcı** | : | Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen gerçek veya tüzel kişilerdir. |
| **İmha** | : | Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir. |
| **Karartma** | : | Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işlemlerdir. |
| **Kayıt Ortamı** | : | Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamdır. |
| **Matbu Ortamlar** | : | Verilerin kâğıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır. |
| **Yerel Dijital Ortamlar** | : | Şirket bünyesinde yer alan sunucular, sabit ya da taşınabilir diskler, optik diskler gibi sair dijital ortamlardır. |
| **Bulut Ortamlar** | : | Şirket bünyesinde yer almamakla birlikte, Şirket'in kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır. |
| **Maskeleme** | : | Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemlerdir. |
| **Veri Kayıt Sistemi** | : | Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir. |
| **Kişisel Verilerin İşlenmesi ve Korunması Politikası** | : | Credence tarafından oluşturulan ve web sitesinde paylaşılan, kişisel verilerin işlenme ve korunma esaslarını tanımlayan politika dokümanıdır. |

## 4. SORUMLULUK

Bu politikanın denetlenmesinden ve güncellenmesinden Şirket yönetimi, uygulanmasından tüm çalışanlar ve veri işleme sürecine katılan diğer paydaşlar sorumludur.

## 5. UYGULAMA

### 5.1. Ortamlar ve Güvenlik Tedbirleri

Şirket nezdinde saklanan kişisel veriler, ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur.

Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibariyle matbu ortamlar, yerel dijital ortamlar ve bulut ortamlardır.

Ancak, bir kısım veriler sahip oldukları özel nitelikler ya da hukuki yükümlülüklerimiz nedeniyle tanımlanmış ortamlardan farklı bir ortamda tutulabilir. Şirket her koşulda veri sorumlusu sıfatıyla hareket etmekte ve kişisel

verileri Kanun'a, Kişisel Verilerin İşlenmesi ve Korunması Politikası'na ve işbu Kişisel Veri Saklama ve İmha Politikası'na uygun olarak işlemek ve korumaktadır.

Kanun'un 12'nci maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin İşlenmesi ve Korunması Politikası hükümlerinin uygulanmasına ilişkin şirket içi denetimler yapmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilir. Şirket, kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak gerekli tüm teknik ve idari tedbirleri almaktadır.

İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi kapsamında ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düştüğü ölçüde aşağıdaki idari ve teknik tedbirleri kapsar.

**5.1.1.Teknik Tedbirler**

Şirket, kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki teknik tedbirleri almaktadır:

- Kişisel verilerin tutulduğu ortamlarda yalnızca teknolojik gelişmelere uygun güncel ve güvenli sistemler kullanılmaktadır.
- Kişisel verilerin tutulduğu ortamlara yönelik güvenlik sistemleri kullanılmaktadır.
- Bilişim sistemleri üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri ve araştırmaları yapılmakta, yapılan test ve araştırmaların sonucunda tespit edilen mevcut ya da muhtemel risk teşkil eden hususlar giderilmektedir.
- Kişisel verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmekte ve tüm erişimler kayıt altına alınmaktadır.
- Şirket bünyesinde kişisel verilerin tutulduğu ortamların güvenliğini sağlamak üzere yeterli teknik personel bulundurmaktadır.

**5.1.2 İdari Tedbirler**

Şirket, kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki idari tedbirleri almaktadır:

- Kişisel verilere erişimi olan tüm Şirket çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapılmaktadır.
- Bilgi güvenliği, özel hayatın gizliliği ve kişisel verilerin korunması alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alınmaktadır.
- Kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalanmakta, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özen gösterilmektedir.

### 5.1.3. Şirket İçi Denetim

Şirket, Kanun'un 12'nci maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin İşlenmesi ve Korunması Politikası hükümlerinin uygulanmasına ilişkin şirket içi denetimler yapmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilir.

Denetim sırasında ya da sair bir şekilde Şirket sorumluluğunda bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması hâlinde, Şirket bu durumu en kısa sürede ilgilisine ve Kurula bildirir.

### 5.2. Kişisel Verilerin Saklanması

Şirket bünyesinde tutulan kişisel veriler Kanun uyarınca, aşağıda belirtilen amaç ve sürelerde saklanmaktadır.

| KİŞİSEL VERİ | SÜRE / AMAÇ |
|---|---|
| **Özlük Bilgisi** | **1.** Hizmet akdi süresince iş kazası/meslek hastalığına maruz kalmamış çalışanlar açısından hizmet ilişkisinin sona erdiği tarihten itibaren 5 yıl süreyle muhafaza edilir. Süre, fasılalı çalışmalarda son çalışma döneminin sona erdiği tarihten itibaren işlemeye başlar.<br>**2.** Hizmet akdi süresince iş kazası/meslek hastalığına maruz kalmış yahut bu riski taşıyan çalışanlar açısından özlük kayıtları, iş kazası tarihi/meslek hastalığı tespit tarihini müteakip 10 yıl süreyle saklanabilir. Bu durumda saklama süresi olarak uzun olan süre(hizmet ilişkisinin hitamından itibaren 5 yıl / kaza-tespit tarihinden itibaren 10 yıl) uygulanır. |
| **Çalışanların Kişisel Sağlık Dosyaları** | Çalışanın işten ayrılma tarihinden itibaren 15 yıl süreyle çalışanların kişisel sağlık dosyaları saklanır. |
| **Çalışan Adayı Bilgileri** | En fazla 2 yıl olmak üzere özgeçmişin güncelliğini kaybedeceği süre kadar saklanır. |
| **Müşteri Bilgileri** | Müşteri Bilgilerinden, Türk Ticaret Kanunu md.82 uyarınca ticari defter ve kayıtlara dayanak teşkil eden faturaların düzenlenmesine esas bilgiler anılan kanun maddesi gereği 10 yıl süre ile, bunun dışındaki Müşteri Bilgileri ise işlendikleri amaç için gerekli olan süre kadar saklanır. |
| **Ziyaretçi Bilgileri** | 2 yıl süre ile saklanır. |
| **İş Ortağı/Çözüm Ortağı/Danışman Bilgileri** | İş Ortağı/Çözüm Ortağı/Danışmanın, Şirket ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 uyarınca 10 yıl süre ile saklanır. |
| **Şirket'in İşbirliği İçinde Olduğu Kurum/Firmalar Tarafından Şirket ile Paylaşılan Kişisel Veriler** | Şirketin İşbirliği İçinde Olduğu Kurum/Firmaların Şirketin ile olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 uyarınca 10 yıl süre ile saklanır. |
| **Potansiyel Müşteri Bilgileri** | 2 yıl süre ile saklanır. |

* Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.

### 5.3. Kişisel Verilerin İmhası

#### 5.3.1. İmha Nedenleri

Şirket bünyesinde bulunan kişisel veriler ilgili kişinin talebi halinde ya da Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenlerin ortadan kalkması halinde resen işbu imha politikası uyarınca silinir/yok edilir.

Kanun'un 5'nci ve 6'ncı maddelerinde sayılan nedenler:

**a)** Kanunlarda açıkça öngörülmesi.
**b)** Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
**c)** Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
**d)** Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
**e)** İlgili kişinin kendisi tarafından alenileştirilmiş olması.
**f)** Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.
**g)** İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

#### 5.3.2. İmha Yöntemleri

Şirket, Kanuna ve sair mevzuatı ile Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re'sen siler yok eder.

Şirket tarafından en çok kullanılan silme, yok etme ve anonim hale getirme teknikleri aşağıda sıralanmaktadır:

##### 5.3.2.1. Silme Yöntemleri

Matbu ortamda tutulan Kişisel Veriler için kullanılan silme yöntemi karartmadır. Bulut ve yerel dijital ortamda tutulan Kişisel Veriler için verilerin bir daha geri getirilemeyecek şekilde komutlarla veya yardımcı yazılımlarla silinmesidir.

#### 5.3.2. 2. Yok Etme Yöntemleri

Matbu ortamlarda tutulan Kişisel Veriler evrak imha makinaları ile bir daha bir araya getirilemeyecek şekilde yok edilirler. Yerel dijital ortamda tutulan Kişisel Veriler yok edilmek istenildiğinde, Kişisel veri barındıran optik ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Bulut ortamında saklanan Kişisel Veriler için dijital yok etme yöntemleri kullanılır.

### 5.3.3. İmha Süreleri

Şirket, Kanun, ilgili mevzuat, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve işbu Kişisel Verileri Saklama ve İmha Politikası uyarınca sorumlu olduğu kişisel verileri silme, yok etme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler / yok eder.

İlgili kişi, Kanunun 13'ncü maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde:

**a)** Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder Şirket'in talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin İşlenmesi ve Korunması Politikasına uygun olarak yapmış olması gerekir. Şirket, her durumda yapılan işlemle ilgili ilgili kişiye bilgi verir.

**b)** Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından Kanunun 13'ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

### 5.3.4. Periyodik İmha

Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda; Şirket işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek bir işlemle siler, yok eder.

Periyodik imha süreçleri ilk kez 31.08.2018 tarihinde başlar ve her 6 (altı) ayda bir tekrar eder.

#### 5.3.4.1. İmha İşleminin Hukuka Uygunluğu

Şirket, gerek talep üzerine gerekse periyodik imha süreçlerinde re'sen gerçekleştirdiği imha işlemlerini Kanuna, sair mevzuata, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve işbu Kişisel Veri Saklama ve İmha Politikasına uygun olarak yapar.

Şirket, imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla bir takım idari ve teknik tedbirler almaktadır.

##### 5.3.4.1.1. Teknik Tedbirler

- Şirket, işbu politikada yer alan imha yöntemine uygun teknik araç ve ekipman bulundurur.
- Şirket, imha işlemlerinin yapıldığı yerin güvenliğini sağlar.
- Şirket, imha işlemini yapan kişilerin erişim kayıtlarını tutar.
- Şirket, imha işlemini yapacak yetkin ve tecrübeli elemanlar istihdam eder ya da gerektiğinde yetkin üçüncü kişilerden hizmet alır.

**5.3.4.1.1. İdari Tedbirler**

- Şirket, imha işlemini yapacak çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapar.
- Şirket, bilgi güvenliği, özel hayatın gizliliği, kişisel verilerin korunması ve güvenli imha teknikleri alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alır.
- Şirket, teknik ya da hukuki gereklilikler nedeniyle imha işlemini üçüncü kişilere yaptırdığı durumlarda ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalar, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.
- Şirket, imha işlemlerinin hukuka ve işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen şart ve yükümlülüklere uygun olarak yapılıp yapılmadığını düzenli olarak denetler, gereken aksiyonları alır.
- Şirket, kişisel verilerin silinmesi, yok edilmesi ilgili yapılan bütün işlemleri kayıt altına alır ve söz konusu kayıtları, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklar.

## 6. KİŞİSEL VERİ KOMİTESİ

Şirket bünyesinde Kişisel Veri Komitesi "Bilgi Güvenliği Komitesi" üyelerinden oluşmaktadır. Kişisel Veri Komitesi, ilgili kişilerin verilerinin hukuka, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve Kişisel Veri Saklama ve İmha Politikasına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir.

Kişisel Veri Komitesi bir yönetici, bir idari uzman ve bir teknik uzman olmak üzere üç kişiden oluşur.

Kişisel Veri Komitesinde görevli Şirket çalışanlarının unvanları ve görev tanımları aşağıda belirtilmiştir:

| Unvan | | Görev Tanımı |
|---|---|---|
| **Kişisel Veri Komitesi Yöneticisi** | : | Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; Kanun, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür. |
| **Teknik ve İdari Uzmanlar** | : | İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Komitesi Yöneticisine raporlanmasından; Kişisel Veri Komitesi Yöneticisi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Komitesi Yöneticisinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Komitesi Yöneticisine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur. |

## 7. GÜNCELLEME VE UYUM

Şirket, Kanunda yapılan değişiklikler nedeniyle, Kurum kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda Kişisel Verilerin İşlenmesi ve Korunması Politikasında ya da işbu Kişisel Veri Saklama ve İmha Politikasında değişiklik yapma hakkını saklı tutar.

İşbu Kişisel Veri Saklama ve İmha Politikasında yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar politikanın sonunda açıklanır.

### 7.1. Değişiklik Notları

12.05.2018 : Kişisel Veri Saklama ve İmha Politikası yayınlanmıştır.

*Daha eski tarihli bir değişiklik bulunmamaktadır.*