KONYA HAZIR BETON SANAYİ VE TİCARET ANONİM ŞİRKETİ
("Şirket")
YÖNETİM KURULU KARARI

Karar Tarihi :
Karar No :
Konu : 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca Şirket'in kişisel verilerin korunması politikasının onaylanması

Şirket Yönetim Kurulu aşağıdaki hususları görüşerek karara bağlamıştır:

1. 6698 sayılı Kişisel Verilerin Korunması Kanunu ("**Kanun**") ve kişisel verilerin korunmasına yönelik ilgili diğer düzenlemeler (birlikte "**KVK Düzenlemeleri**" olarak anılır) kapsamında, ekte yer alan Şirket Kişisel Verilerin Korunması Politikasının ("**Politika**") ve ekinde yer alan prosedürlerin ("**KVK Prosedürleri**") birinci versiyonlarının 7 Nisan 2016 tarihi itibariyle bağlayıcı olmak üzere onaylanmasına, Politika'nın tüm çalışanlarımıza e-posta ve sair kanallardan duyurulmasına ve erişimlerine sunulmasına ayrıca www.konyahazirbeton.com.tr internet sitemiz üzerinden Şirket dışı tüm ilgililere duyurulmasına,

oybirliği ile karar verilmiştir.

Ek - Kişisel Verilerin Korunması Politikası

Doküman Bilgileri	
Doküman Adı:	Kişisel Verilerin Korunması Politikası
Doküman İçeriği:	Bu politikanın amacı, Konya Hazır Beton Sanayi ve Ticaret Anonim Şirketi (“**Şirket**”) tarafından, Kişisel Verilerin korunmasına yönelik yöntem ve süreçlere ilişkin esasları belirlemektir.
Yürürlük Tarihi:	7 Nisan 2016
Revizyon No:	İlk yayındır.
Referans / Gerekçe	6698 sayılı Kişisel Verilerin Korunması Kanunu
Onaylayan:	Şirket Yönetim Kurulu

KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

I. GİRİŞ

İşbu Kişisel Verilerin Korunması Politikası ("**Politika**"), Konya Hazır Beton Sanayi ve Ticaret Anonim Şirketi ("**Şirket**" veya "**Veri Sorumlusu**") 6698 Sayılı Kişisel Verilerin Korunması Kanunu başta olmak üzere ilgili mevzuat hükümleri uyarınca Kişisel Verileri korumaya yönelik yükümlülüklerini yerine getirirken ve Kişisel Verileri işlerken Şirket içerisinde ve/veya Şirket tarafından uyulması gereken esasları belirlemektedir.

Veri Sorumlusu, kendi bünyesinde bulunan Kişisel Veriler bakımından işbu Politikaya ve Politikaya bağlı olarak uygulanacak prosedürlere uygun davranmayı taahhüt eder.

II. POLİTİKANIN AMACI

İşbu Politikanın temel amacı, Veri Sorumlusu tarafından Kişisel Verilerin işlenmesine ve korunmasına yönelik yöntem ve süreçlere ilişkin esasları belirlemektir.

III. POLİTİKANIN KAPSAMI

İşbu Politika; Veri Sorumlusunun işlemekte olduğu Kişisel Verilere yönelik tüm faaliyetleri kapsar ve söz konusu faaliyetlere uygulanır. İşbu Politika Kişisel Veri niteliği taşımayan verilere uygulanmaz.

Yürürlükte bulunan mevzuat ve Politika arasında uyumsuzluk bulunması durumunda, mevzuat hükümleri öncelikli olarak uygulanacaktır.

IV. TANIMLAR

İşbu Politikada geçen tanımlar aşağıdaki anlamları ihtiva eder;

"Açık Rıza" Belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür iradeyle açıklananı rızayı ifade eder.

"Anonim Hale Getirme" Kişisel Verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini ifade eder.

"**Başvuru Formu**" Veri Öznelerinin haklarını kullanmak için Veri Sorumlusuna yapacakları başvuruyu içeren başvuru formunu ifade eder.

"Kişisel Sağlık Verisi" 20.10.2016 tarih ve 29863 sayılı Resmî Gazetede yayımlanan Kişisel Sağlık Verilerin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik kapsamında belirtildiği şekilde kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü sağlık bilgisini ifade eder.

"Kişisel Veri" Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder (işbu Politika kapsamında "Kişisel Veri" ifadesi uygun olduğu ölçüde aşağıda tanımlanan "Özel Nitelikli Kişisel Veriler" ile "Kişisel Sağlık Verileri"ni de kapsayacaktır).

"Kişisel Veri İşleme" 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 veri üzerinde yapılan her türlü işlemi ifade eder.

"Kurul" Kişisel Verileri Koruma Kurulunu ifade eder.

"**Kurum**" Kişisel Verileri Koruma Kurumunu ifade eder.

"KVKK" 6698 sayılı Kişisel Verilerin Korunması Kanununu ifade eder.

"KVK Düzenlemeleri" 6698 sayılı Kişisel Verilerin Korunması Kanunu ile Kişisel Verilerin korunmasına yönelik ilgili diğer mevzuatı, düzenleyici ve denetleyici otoriteler, mahkemeler ve diğer resmi makamlar tarafından verilen, bağlayıcı kararları, ilke kararlarını, hükümleri, talimatları ile verilerin korunmasına yönelik uygulanabilir uluslararası anlaşmaları ve diğer her türlü mevzuatı ifade eder.

"**KVK Prosedürleri**" Yönetim Kurulu tarafından onaylanarak yürürlüğe giren ve Veri Sorumlusu'nun, çalışanların, işbu Politika kapsamında uyması gereken yükümlülükleri belirleyen prosedürleri ifade eder.

"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 verileri ifade eder.

"Silme veya Silinme" Kişisel Verilerin geri döndürülemez biçimde imha edilmesini yahut yok edilmesini ifade eder.

"Veri Envanteri" Veri Sorumlusunun Kişisel Veri İşleme faaliyetlerine yönelik olarak Kişisel Veri İşleme süreç ve yöntemleri, Kişisel Veri İşleme amaçları, veri kategorisi, Kişisel Verilerin aktarıldığı üçüncü kişiler vb. bilgileri ihtiva eden envanteri ifade eder.

"Veri İşleyen" Veri Sorumlusu tarafından yetki alarak, Veri Sorumlusu adına Kişisel Verileri işleyen gerçek veya tüzel kişiyi ifade eder.

"Veri Öznesi" Kişisel Verileri Veri Sorumlusu tarafından veya Veri Sorumlusu adına işleme sokulan tüm gerçek kişileri ifade eder.

"Veri Sorumlusu" Kişisel Verileri İşleme amaçları ve İşleme yollarını belirterek işleyen, veri kayıt sisteminin kurulması ve yönetilmesi sorumluluğu bulunan gerçek veya tüzel kişiyi ifade eder. İşbu Politika kapsamında Veri Sorumlusu Şirket'i ifade etmektedir.

"Yönetmelik" 20.10.2016 tarih ve 29863 sayılı Resmî Gazetede yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'i ifade eder.

V. KİŞİSEL VERİ İŞLEMENİN İLKELERİ

(i) Kişisel Verilerin Hukuka ve Dürüstlük Kurallarına Uygunluk Olarak İşlenmesi

Kişisel Veriler, Veri Sorumlusu tarafından hukuka ve dürüstlük kurallarına uygun ve ölçülülük esasına dayalı olarak işlenir.

(ii) Kişisel Verilerin Doğru ve Gerektiğinde Güncel Olması için Gerekli Önlemlerin Alınması

Veri Sorumlusu, Kişisel Verilerin eksiksiz, doğru ve güncel olması için her türlü gerekli önlemleri alır. Veri Öznesinin Kişisel Verilere yönelik değişiklik talep etmesi durumunda ilgili Kişisel Verileri günceller.

(iii) Kişisel Verilerin Belirli, Meşru ve Açık Amaçlar Doğrultusunda İşlenmesi

Kişisel Verilerin İşlenmesinden önce Veri Sorumlusu tarafından Kişisel Verilerin hangi amaçla İşleneceği belirlenir. Bu kapsamda, Veri Öznesi KVK Düzenlemeleri kapsamında aydınlatılır ve gereken hallerde Açık Rızaları alınır.

(iv) Kişisel Verilerin İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olması

Veri Sorumlusu, Kişisel Verileri yalnızca KVK Düzenlemeleri kapsamında istisnai hallerde (KVKK Madde 5.2 ve Madde 6.3) veya Veri Öznesinden alınan Açık Rıza kapsamındaki amaç doğrultusunda (KVKK Madde 5.1 ve Madde 6.2) ve ölçülülük esasına uygun olarak işler. Veri Sorumlusu, Kişisel Verileri belirlenen amaçların gerçekleştirilebilmesine elverişli bir biçimde işler ve amacın gerçekleştirilmesiyle ilgili olmayan veya ihtiyaç duyulmayan Kişisel Verileri işlemekten kaçınır.

(v) Kişisel Verilerin Gerektiği Kadar Muhafaza Edilmesi ve Sonrasında Silinmesi

Veri Sorumlusu, Kişisel Verileri amaca uygun olarak gerektiği kadar muhafaza eder. Veri Sorumlusu, KVK Düzenlemelerinde öngörülen veya Kişisel Veri İşleme amacının gerektirdiği süreden daha uzun bir süreyle Kişisel Verileri muhafaza etmek istenmesi halinde KVK Düzenlemelerinde belirtilen yükümlülüklere uygun davranır.

Kişisel Veri İşleme amacının gerektirdiği süre sona erdikten sonra Kişisel Veriler Silinir veya Anonim Hale Getirilir. Veri Sorumlusunun Kişisel Verileri aktardığı üçüncü kişilerin de Kişisel Verileri Silmesi yahut Anonim Hale Getirmesi sağlanır. Veri Sorumlusu, Silme ve Anonim Hale Getirme süreçlerinin işletir ve bu kapsamda gerekli politika ve/veya prosedürleri ayrıca oluşturur.

VI. KİŞİSEL VERİLERİN İŞLENMESİ

Veri Sorumlusu Kişisel Verilerin İşlenmesi sürecinde KVKK ve KVK Düzenlemelerine uygun hareket etmekte, Kişisel Veri İşleme ilkelerine uymaktadır. Kişisel Veriler Veri Sorumlusu tarafından ancak aşağıda belirtilen usul ve esaslar kapsamında işlenebilir.

6.1. Açık Rıza

Kişisel Veriler, Veri Öznelerine Aydınlatma Yükümlülüğünün yerine getirilmesi çerçevesinde yapılacak bilgilendirme sonrası ve Veri Öznelerinin Açık Rıza vermesi halinde işlenir.

Aydınlatma Yükümlülüğü çerçevesinde Açık Rıza alınmadan önce Veri Öznelerine hakları bildirilir.

Veri Öznesinden Açık Rızası KVK Düzenlemelerine uygun yöntemlerle alınır. Açık Rızalar ispatlanabilir şekilde Veri Sorumlusu tarafından KVK Düzenlemeleri kapsamında gereken süre ile muhafaza edilir.

Veri Sorumlusu tüm Kişisel Veri İşleme süreçlerin bakımından Aydınlatma Yükümlülüğü'nün yerine getirilmesini ve gerektiğinde Açık Rızanın alınmasını ve muhafazasını sağlamakla yükümlüdür. Kişisel Veri İşleyen tüm departman çalışanları KVKK, KVKK Düzenlemeleri, Veri Sorumlusu'nun talimatlarına, işbu Politika'ya ve KVK Prosedürlerine uymakla yükümlüdür.

6.2. Kişisel Verilerin Açık Rıza Alınmaksızın İşlenmesi

KVK Düzenlemeleri kapsamında Açık Rıza alınmaksızın Kişisel Verilerin İşlenmesinin öngörüldüğü durumlarda (KVKK Madde 5.2), Veri Sorumlusu, Veri Öznesinin Açık Rızasını almaksızın Kişisel Verileri işleyebilir. Kişisel Verilerin bu şekilde işlenmesi durumunda Veri Sorumlusu KVK Düzenlemelerinin çizdiği sınırlar çerçevesinde Kişisel Verileri işler. Bu kapsamda:

(i) Veri Öznesinin Kişisel Verileri, kanunlarda açıkça öngörülmesi durumunda Veri Sorumlusu tarafından Açık Rıza olmaksızın işlenebilir.

(ii) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan Veri Öznesinin ve/veya Veri Öznesi dışındaki bir kişinin hayatını veya beden bütünlüğünün korunması için Kişisel Veriler Veri Sorumlusu tarafından Açık Rıza olmaksızın işlenebilir.

(iii) Bir sözleşmenin kurulması, uygulanması veya ifasıyla doğrudan doğruya ilgili olması şartları sağlanıyorsa, sözleşmenin taraflarına ait Kişisel Veriler Veri Öznelerinin Açık Rızaları olmadan Veri Sorumlusu tarafından işlenebilir.

(iv) Kişisel Verilerin işlenmesi Veri Sorumlusunun hukuki yükümlülüğünü yerine getirmesi için zorunluysa Kişisel Veriler Veri Öznelerinin Açık Rızaları olmadan Veri Sorumlusu tarafından işlenebilir.

(v) Veri Öznesi tarafından alenileştirilmiş olan Kişisel Veriler Açık Rıza alınmaksızın Veri Sorumlusu tarafından işlenebilir.

(vi) Kişisel Verilerin bir hakkın tesisi, kullanılması veya korunması için işlenmesi zorunlu ise Kişisel Veriler Açık Rıza alınmaksızın Veri Sorumlusu tarafından işlenebilir.

(vii) Veri Öznesinin temel hak ve özgürlüklerine zarar vermemek kaydıyla Veri Sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması durumunda olan Kişisel Veriler Açık Rıza alınmaksızın Veri Sorumlusu tarafından işlenebilir.

VII. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ

Özel Nitelikli Kişisel Veriler yalnızca;

(i) Veri Öznesinin Açık Rızasının bulunması veya,

(ii) Veri Öznesinin Açık Rızası yok ise,

- Cinsel hayat ve kişisel sağlık verileri dışındaki Özel Nitelikli Kişisel Veriler bakımından kanunlarda açıkça işlenmelerinin zorunlu tutulması halinde,
- Sağlık ve cinsel hayata ilişkin Kişisel Veriler ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla sır saklama yükümlülüğü altında bulunan kişiler (örnek: Şirket hekimi) veya yetkili kurum ve kuruluşlar tarafından Açık Rıza almaksızın işlenebilir.

Özel Nitelikli Kişisel Veriler işlenirken, Kurul tarafından belirlenen önlemler alınır. Veri Sorumlusu Özel Nitelikli Kişisel Verilerin işlenmesi ile ilgili ek politika veya prosedürler tesis edip, yayınlayabilir.

Özel Nitelikli Kişisel Verilerin İşlenmesini gerektiren her durumda ilgili çalışan tarafından Veri Sorumlusu bilgilendirilir. Bir verinin Özel Nitelikli Kişisel Veri olup olmadığı anlaşılabilir değil ise ilgili departman tarafından Veri Sorumlusundan görüş alınır.

VIII. KİŞİSEL VERİLERİN AKTARILMASI VE KİŞİSEL VERİLERİN ÜÇÜNCÜ KİŞİLER TARAFINDAN İŞLENMESİ

Veri Sorumlusu, Kişisel Veri işleme amaçları doğrultusunda gerekli önlemleri alarak Kişisel Verileri yurtiçinde ve/veya yurtdışında bulunan üçüncü bir gerçek ya da tüzel kişiyle KVK Düzenlemelerine uygun şekilde aktarabilir. Veri Sorumlusu bu durumda Kişisel Veri aktardığı üçüncü kişilerin de işbu Politika'ya uymasını sağlar. Bu kapsamda üçüncü kişi ile akdedilen sözleşmelere gerekli koruyucu düzenlemeler eklenir. Her bir çalışan Kişisel Veri aktarımı yapılacak durumda işbu Politika'da yer alan süreci kat etmekle yükümlüdür.

(i) Türkiye'de Bulunan Üçüncü Kişilere Kişisel Veri Aktarım

Kişisel Veriler, KVKK Madde 5.2'de ve Madde 6.3'de belirlenen istisnai hallerde Açık Rıza olmaksızın yahut diğer hallerde Veri Öznesinin Açık Rızası alınmak şartı ile Türkiye'de bulunan üçüncü kişilere Veri Sorumlusu tarafından aktarılabilir.

Veri Sorumlusu, Kişisel Verilerin Türkiye'de üçüncü kişilere aktarımının KVK Düzenlemelerine uygun olmasını sağlar.

(ii) Yurt Dışında Bulunan Üçüncü Kişilere Aktarım

Kişisel Veriler, KVKK Madde 5.2'de ve Madde 6.3'de belirlenen istisnai hallerde Açık Rıza olmaksızın yahut diğer hallerde Veri Öznesinin Açık Rızası alınmak şartı ile (KVKK Madde 5.1 ve Madde 6.2) yurtdışında bulunan üçüncü kişilere Veri Sorumlusu tarafından aktarılabilir.

Kişisel Verilerin KVK Düzenlemelerine uygun olarak Açık Rıza alınmaksızın aktarıldığı durumda ayrıca aktarılacağı yabancı ülke bakımından aşağıdaki koşullardan birinin varlığı gerekir:

- Kişisel Verilerin aktarıldığı yabancı ülkenin Kurul tarafından yeterli korumanın bulunduğu ülkeler statüsünde olması (liste için lütfen Kurul'un güncel listesini takip edin),

- Aktarımın gerçekleşecek olduğu yabancı ülkenin Kurul'un güvenli ülkeler listesinde yer almaması halinde Veri Sorumlusunun ve ilgili ülkedeki veri sorumlularının yeterli korumanın sağlanacağına ilişkin yazılı taahhütte bulunarak Kuruldan izin alması.

Veri Sorumlusu, Kişisel Verilerin Yurt dışında üçüncü kişilere aktarımının KVK Düzenlemelerine uygun olmasını sağlar.

IX. AYDINLATMA YÜKÜMLÜLÜĞÜ

Veri Sorumlusu, KVKK'nın 10. Maddesine uygun olarak, Kişisel Verilerin İşlenmesinden önce Veri Öznelerini aydınlatır. Bu kapsamda Veri Sorumlusu, Kişisel Verilerin elde edilmesi sırasında Aydınlatma Yükümlülüğünü yerine getirir. Aydınlatma Yükümlülüğü kapsamında Veri Öznelerine yapılacak olan bildirim sırasıyla şu unsurları içerir: **(i)** Veri Sorumlusunun ve varsa temsilcisinin kimliği, **(ii)** Kişisel Verilerin hangi amaçla işleneceği, **(iii)** İşlenen Kişisel Verilerin kimlere ve hangi amaçla aktarılabileceği, **(iv)** Kişisel Veri toplamanın yöntemi ve hukuki sebebi ve **(v)** Veri Öznelerinin hakları.

Veri Sorumlusu, Türkiye Cumhuriyeti Anayasası'nın 20. ve KVKK'nın 11. maddesine uygun olarak Veri Öznesinin bilgi talep etmesi halinde gerekli bilgilendirmeyi yapar.

Veri Sorumlusu, Kişisel Verilerin İşlenmesinden önce gerekli Aydınlatma Yükümlülüğünün yerine getirilmesini sağlamaktan ilgili süreci takip eden çalışan ile birlikte sorumludur.

Veri İşleyenin Şirket haricinde üçüncü bir kişi olması halinde, üçüncü kişinin yukarıda belirtilen yükümlülüklere uygun davranacağı yazılı bir sözleşme ile Kişisel Veri İşlemeye başlanmadan önce üçüncü kişi tarafından taahhüt edilmelidir. Her bir çalışan Şirket'e üçüncü bir kişi tarafından Kişisel Veri aktarımı yapılan durumda işbu Politika'da yer alan süreci kat etmekle yükümlüdür.

X. KİŞİSEL VERİLERİN MUHAFAZA EDİLMESİ, SİLİNMESİ, YOK EDİLMESİ VE ANONİM HALE GETİRİLMESİ

Veri Sorumlusu, KVKK ve diğer kanun hükümlerine uygun olarak işlemekte olduğu Kişisel Verileri ilgili mevzuatlarda öngörülen sürelere uygun şekilde ve her halükârda Veri Sorumlusunun meşru amaçlar ortadan kalkmadığı müddetçe muhafaza etmektedir.

Veri Sorumlusu yukarıda belirtilen süreler sona erdiğinde Kişisel Verileri re'sen veya Veri Öznesinin talebi üzerine Siler yahut Anonim Hale Getirir. Bu kapsamda, Veri Sorumlusu ilgili yükümlülüğünü yerine

getirmek üzere Şirket içerisinde gerekli teknik ve idari tedbirleri alır. Veri Sorumlusu Kişisel Verilerin Silme veya Anonim Hale Getirilmesi ile ilgili ek politika veya prosedürler tesis edip, yayınlayabilir.

XI. VERİ ÖZNELERİNİN HAKLARI

Veri Sorumlusu Kişisel Verisini elinde bulundurduğu Veri Öznelerinin aşağıda belirtilen taleplerine KVK Düzenlemelerine uygun şekilde cevap verir.

- **(i)** Kişisel Verilerini işleyip işlemediği öğrenme,
- **(ii)** Kişisel Verileri işlenmişse buna ilişkin bilgi talep etme,
- **(iii)** Kişisel Verilerin işleme amacını ve bunların amacına uygun kullanıp kullanılmadığını öğrenme,
- **(iv)** Şirket'in Kişisel Verilerini aktardığı yurt içinde veya yurt dışında üçüncü kişileri öğrenme,
- **(v)** Kişisel verilerinin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- **(vi)** KVKK ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel verilerin silinmesini veya yok edilmesini isteme ve bu kapsamda yapılan işlemin kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- **(vii)** İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- **(viii)** Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme.

Veri Öznelerinin yukarıda belirtilen haklarını kullanmakla ilgili taleplerini kimliklerini tespit edici bilgi ve belgelerler birlikte www.konyahazirbeton.com.tr adresinde yer alan Başvuru Formu'nu doldurup, Veri Sorumlusu ile ilgili aşağıda verilen ve zaman zaman değişebilecek olan e-posta adresine güvenli elektronik imzalı olarak yahut yine aşağıda yer alan ve zaman zaman değişebilecek olan posta adresine ile ıslak imzalı bir dilekçe ile elden teslim edebilir, iadeli taahhütlü posta ya da noter aracılığıyla gönderebilir.

Veri Sorumlusu: Konya Hazır Beton Sanayi ve Ticaret Anonim Şirketi
E-posta: konyahazirbeton@hs03.kep.tr
Posta: Horozluhan Mah. Cihan Sok.No:15 Selçuklu/Konya

Veri Öznelerinin yukarıda sıralanan haklarına ilişkin taleplerini yazılı olarak Veri Sorumlusuna iletmeleri durumunda Veri Sorumlusu talebin niteliğine göre talebi en geç otuz gün içinde ücretsiz olarak sonuçlandırır. Ancak, Kurul tarafından bir ücret öngörülmesi hâlinde, Veri Sorumlusu tarafından Kurul tarafından belirlenen tarifedeki ücret alınır.

XII. VERİ YÖNETİMİ VE GÜVENLİĞİ

Veri Sorumlusu tarafından KVKK Madde 12 uyarınca Kişisel Verilerin hukuka aykırı işlenmesini önlemek, kişisel verilere hukuka aykırı olarak erişilmesini önlemek ve Kişisel Verilerin muhafazasını sağlamak başta olmak üzere "veri güvenliğini" sağlamaya yönelik aşağıda belirtilenler dahil olmak üzere ve ilgili sair mevzuat hükümleri saklı tutulmak suretiyle gerekli teknik ve idari tedbirler alınır.

- **(i)** Kişisel Verilerin KVKK, ilgili mevzuat, işbu Politika ve KVK Prosedürlerine uygun şekilde korunmasından ilgili sürece müdahil olan tüm çalışanlar müteselsilen sorumludur.
- **(ii)** Veri Sorumlusu tarafından Kişisel Veri İşleme faaliyetleri teknolojik imkanlar ve uygulama maliyetine göre teknik sistemlerle denetlenmektedir.
- **(iii)** Kişisel Veri İşleme faaliyetlerine yönelik teknik konularda bilgili personel istihdam edilmektedir.

(iv) Şirket çalışanları, Kişisel Verilerin korunmasına ve hukuka uygun olarak işlenmesine yönelik olarak bilgilendirilmekte ve eğitilmektedir.

(v) Şirket'te Kişisel Verilere erişmesi gereken çalışanların söz konusu Kişisel Verilere erişimini sağlamak adına gerekli KVK Prosedürü oluşturulur.

(vi) Şirket çalışanları, Kişisel Verilere üzerinde yalnızca kendilerine tanımlanan yetki dâhilinde ve ilgili KVK Prosedürü'ne uygun olarak erişebilir.

(vii) Şirket çalışanları ile akdedilen sözleşmelere Kişisel Verilerin korunmasına ilişkin gerekli hükümler eklenmekte ve bu konuda çalışanların farkındalığı artırılmaktadır.

(viii) Şirket, çalışanın Kişisel Verilerin güvenliğinin yeterince sağlanmadığı şüphesinde olması yahut böyle bir güvenlik açığını tespitte bulunması halinde derhal durumu Veri Sorumlusu'na bildirir.

(ix) Kişisel Verilerin güvenliğine yönelik detaylı KVK Prosedürü Veri Sorumlusu tarafından oluşturulur.

(x) Kendisine Şirket cihazı tahsis edilen her kişi, kendi kullanımına tahsis edilen cihazlarının güvenliğinden sorumludur.

(xi) Her Şirket çalışanı veya Şirket bünyesinde çalışan kişi kendi sorumluluk alanında yer alan fiziki dosyaların güvenliğinden sorumludur.

(xii) KVK Düzenlemeleri kapsamında Kişisel Verilerin güvenliği için talep edilen veya ek olarak talep edilecek olan güvenlik önlemleri olması durumunda tüm çalışanlar ek güvenlik önlemlerine uymak ve bu güvenlik önlemlerinin sürekliliğini sağlamak ile yükümlüdür.

(xiii) Şirket'te Kişisel Verilerin güvenli ortamlarda saklanması teknolojik gelişmelere uygun olarak virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar kurulmaktadır.

(xiv) Şirkette Kişisel Verilerin kaybolmasını yahut zarar görmesini engellemek üzere yedekleme programları kullanılmakta ve yeterli düzeyde güvenlik önlemleri alınmaktadır.

(xv) Şirket içerisindeki bir departman Özel Nitelikli Kişisel Veri İşliyorsa, bu departman, Veri Sorumlusu tarafından işledikleri Kişisel Verilerin önemi, güvenliği ve gizliliği hakkında bilgilendirilir ve ilgili departman Veri Sorumlusunun talimatlarına uygun hareket ederler. Özel Nitelikli Kişisel Verilere erişim yetkisi yalnızca sınırlı çalışanlara verilir ve bunların listesi ve takibi Veri Sorumlusu tarafından yapılır.

(xvi) Şirket içerisinde işlenen Kişisel Verilerin tamamı Şirket tarafından "Gizli Bilgi" olarak kabul edilir.

(xvii) Şirket çalışanları, Kişisel Verilerin güvenliğine ve gizliliğine ilişkin yükümlülüklerinin, iş ilişkisinin sona ermesinden sonra da devam edeceği konusunda bilgilendirilmiş ve Şirket çalışanlarından bu kurallara uymaları yönünde taahhüt alınmıştır.

XIII. EĞİTİM

Veri Sorumlusu Kişisel Verilerin korunması konusunda çalışanlarına Politika ve ekinde yer alan KVK Prosedürleri ile KVKK Düzenlemeleri kapsamında gerekli eğitimleri verir.

Eğitimlerde Kişisel Sağlık Verileri ve Özel Nitelikli Kişisel Verilerin tanımlarına ve korunmasına yönelik uygulamalara özellikle değinilir.

Şirket çalışanı Kişisel Verilere fiziksel olarak veya bilgisayar ortamında erişiyorsa, Şirket bu çalışanını bu erişimler özelinde (örneğin erişilen bilgisayar programı) eğitim verecektir.

XIV. DENETİM

Veri Sorumlusu, işbu Politika ve KVK Düzenlemelerine Şirket'in tüm çalışanları, departmanları ve yüklenicilerinin uygun hareket ettiğini düzenli olarak hiçbir ön bildirimde bulunmaksızın her zaman ve re'sen denetleme hakkını haizdir ve bu kapsamda gerekli rutin denetimleri yapar.

XV. İHLALLER

Şirket'in her bir çalışanı, KVK Düzenlemelerinde ve işbu Politika kapsamında belirtilen usul ve esaslara aykırı olduğunu düşündüğü iş, işlem yahut eylemi Veri Sorumlusuna raporlar. Bu kapsamda ilgili ihlale yönelik Veri Sorumlusu işbu Politika ve KVK Prosedürleri'ne uygun şekilde eylem planı oluşturur.

Yapılan bilgilendirmeler sonucunda Veri Sorumlusu KVK Düzenlemeleri hükümleri başta olmak üzere konuya ilişkin yürürlükteki mevzuat hükümlerini dikkate alarak ihlale ilişkin Veri Öznesi veya Kurum'a yapılacak bildirimi hazırlar.

XVI. SORUMLULUKLAR

Şirket içerisinde sorumluluklar sırasıyla çalışan, departman, Veri Sorumlusu şeklindedir.

XVII. POLİTİKADA YAPILACAK DEĞİŞİKLİKLER

İşbu Politika KVK Düzenlemelerinin gerektirmesi halinde yahut gerekli görülmesi halinde zaman zaman Yönetim Kurulu onayı ile değiştirilebilir.

Şirket, Politika üzerinde yaptığı değişiklikler incelenebilecek şekilde güncellenen Politika metnini e-posta yolu ile çalışanlarıyla paylaşır ve internet adresi (www.konyahazirbeton.com.tr) üzerinden Veri Öznelerinin erişimine sunar.

XVIII. POLİTİKANIN YÜRÜRLÜK TARİHİ

İşbu Politika 7 Nisan 2016 tarihinden itibaren yürürlükte olmak üzere Şirket Yönetim Kurulu tarafından onaylanmıştır.

KONYA HAZIR BETON SANAYİ VE TİCARET ANONİM ŞİRKETİ
("Company")
BOARD OF DIRECTORS' RESOLUTION

Resolution Date :
Resolution No :
Subject : Approval of the Data Protection Policy of the Company as per Data Protection Law numbered 6698

RESOLUTION

The Board of Directors of the Company unanimously resolved that,

1. Within the scope of the Data Protection Law numbered 6698 ("**Law**") and other related legislation on the protection of personal data, attached first version of the Company Policy on Protection of Personal Data ("**Policy**") and Procedures, which are attached to the Policy ("**Procedures**"), shall be approved to be effective and binding as of 7 April 2016. The Policy will be announced to our employees through e-mail or other methods and will be published on our Company website; www.konyahazirbeton.com.tr, for the review of related parties out of the Company.

Annex – Policy on Protection of Personal Data

[*SIGNATURES*]

Document Details	
Document Title:	Policy on Personal Data Protection
Document Content:	The objective of this policy is to establish the principles in relation to the method and procedures for the protection of Personal Data by Konya Hazır Beton Sanayi ve Ticaret Anonim Şirketi ("**Company**").
Date of Execution:	7 April 2016
Revision No:	First edition.
Reference / Basis	Law on the Protection of Personal Data No. 6698
Approved by:	Company's Board of Directors

POLICY ON PERSONAL DATA PROTECTION

I. INTRODUCTION

This Policy on Personal Data Protection ("**Policy**") establishes the principles to be adhered to by Konya Hazır Beton Sanayi ve Ticaret Anonim Şirketi ("**Company**" or "**Data Controller**") and/or within the organization of the Company during Personal Data processing and the performance of the obligations pursuant to relevant legislations, particularly the Law on Personal Data Protection No. 6698.

The Data Controller undertakes to act in accordance with this Policy and the procedures to be implemented based on the Policy with respect to the Personal Data collected within its own organization.

II. PURPOSE OF THE POLICY

The main purpose of this Policy is to determine the principles in relation to the methods and procedures regarding the processing and the protection of the Personal Data by the Data Controller.

III. SCOPE OF THE POLICY

This Policy covers and applies to all operations related to the Personal Data processed by the Company. This Policy will not apply to data which does not bear the qualification of Personal Data.

In the event of any discrepancy between the applicable laws and this Policy, the applicable laws shall prevail.

IV. DEFINITIONS

The terms used in this Policy shall have the following meanings;

"Explicit Consent" shall mean the consent given with free will and based on being informed about a certain subject.

"Anonymization" shall mean to render the Personal Data impossible to be associated in any manner with a real person identity of whom is identified or identifiable, even in conjunction with other data.

"**Application Form**" shall mean the form to be used by Data Subject to use its rights towards the Data Controller.

"Personal Health Data" shall mean any kind of health information regarding an identified or identifiable real person as stipulated under the Regulation on Processing Personal Health Data and Protecting Its Privacy published in the Official Gazette number 29863, dated 20.10.2016.

"**Personal Data**" shall mean any kind of information regarding an identified or identifiable real person (in the context of this Policy, "Personal Data" shall include "Personal Health Data" and "Sensitive Personal Data" defined below, to the extent applicable).

"**Processing Personal Data**" shall mean any transaction performed on the data, such as obtaining, recording, storing, preserving, altering, reorganizing, disclosing, transferring, acquiring, making obtainable, classifying the personal data or preventing the use of it, by fully or partly automatic means, or by non-automatic means provided that such is a part of a data recording system.

"**Board**" shall mean the Personal Data Protection Board.

"**Authority**" shall mean the Personal Data Protection Authority.

"**LPPD**" shall mean the Law on the Protection of Personal Data No. 6698.

"**PDP Regulations**" shall mean the Law on the Protection of Personal Data No. 6698 and other regulations in relation to the protection of Personal Data, binding decisions, holding decisions, provisions, directives given by regulatory and supervisory authorities, courts and other official authorities and applicable international agreements regarding data protection and any other legislation.

"**PDP Procedures**" shall mean the procedures entering into force upon approval of the Board of Directors, and which establishes the obligations that must be complied by the Data Controller and employees within the scope of this Policy.

"**Sensitive Personal Data**" shall mean the data in relation to race, ethnic origin, political opinion, philosophic belief, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, health, sexual life, imprisonment and security measures as well as biometric and genetic data of individuals.

"**Deletion**" shall mean to delete or destruct the Personal Data in an irreversible manner.

"**Data Inventory**" shall mean the inventory containing information on the Personal Data Processing activities of the Data Controller, such as the Personal Data Processing procedures and methods, purposes of Processing Personal Data, data categories, third parties to whom Personal Data is transferred to, etc.

"**Data Processor**" shall mean real or legal persons which process Personal Data in the name of the Data Controller by receiving authorization from the Data Controller.

"Data Subject" shall mean all real persons Personal Data of whom are processed by or in the name of the Data Controller.

"Data Controller" shall mean real or legal persons who process Personal Data by determining the purposes and methods for Processing, and is responsible for establishing and managing the data recording system. For the purposes of this Policy, the Data Controller shall refer to the Company.

"Regulation" shall mean the Regulation on Processing Personal Health Data and Protecting Its Privacy published in Official Gazette number 29863, dated 20.10.2016.

V. PRINCIPLES OF PROCESSING PERSONAL DATA

(vi) Processing of Personal Data in Accordance with Laws and the Principle of Good Faith

The Personal Data shall be processed by the Data Controller in accordance with laws and the principle of good faith and based on the principle of proportionality.

(vii) Taking Necessary Precautions to Ensure Personal Data is Correct and Up-to-date

The Data Controller shall take all necessary precautions for the Personal Data to be complete, accurate and up-to-date and shall reflect the changes to Personal Data upon the request of the Data Subject.

(viii) Processing of Personal Data for Specific, Legitimate and Explicit Purposes

The purpose for Processing the Personal Data shall be determined by the Data Controller before Processing Personal Data In this context, the Data Subject shall be informed as per the PDP Regulations and Explicit Consent shall be obtained when necessary.

(ix) Relevancy, Adequacy and Proportionality of the Personal Data with the Purposes of Processing

The Data Controller shall only Process the Personal Data pursuant to the exceptional circumstances under the PDP Regulations (LPPD Article 5.2 and Article 6.3) or in line with the purposes of the Explicit Consent obtained from the Data Subject (LPPD Article 5.1 and Article 6.2) and in accordance with the principle of proportionality. Data Controller shall Process the Personal Data in an adequate manner to accomplish the purposes established, and shall refrain from Processing the Personal Data which are irrelevant or unnecessary in relation thereto.

(x) Retaining the Personal Data for the Necessary Period and Deleting Thereafter

The Data Controller shall retain the Personal Data for a necessary period in accordance with their purpose. If the Data Controller intends to retain the Personal Data for a longer period than stipulated under the PDP Regulations or required as per the purposes of the Personal Data Processing, the Company shall act in accordance with the obligations stipulated under the PDP Regulations.

The Personal Data shall be either Deleted or Anonymized, after the end of the period required as per the purposes of the Personal Data Processing. Also, it shall be ensured that the third parties, to whom the Company has transferred Personal Data, Delete or Anonymize such Personal Data. The Data Controller shall carry out the Deletion and Anonymization processes and shall also establish the procedures required in this regard.

VI. PROCESSING OF PERSONAL DATA

The Data Controller shall act in accordance with LPPD and PDP Regulations, and abide by the principles of Personal Data Processing, during Processing Personal Data. Personal Data shall be processed by the Data Controller, only within the scope of the principles and procedures indicated below.

6.1. Explicit Consent

Personal Data shall be processed upon providing information within the framework of performing the Obligation to Inform Data Subjects and where the Data Subject gives his/her Explicit Consent.

In the scope of the Obligation to Inform, before obtaining their Explicit Consent, Data Subjects shall be informed of their rights.

The Explicit Consent of the Data Subject shall be obtained with the methods compatible with the PDP Regulations. Explicit Consent shall be preserved by the Data Controller for the duration required as per the PDP Regulations in a provable manner.

The Data Controller shall fulfill its Obligation to Inform, and if required, obtain and preserve Explicit Consent with respect to any and all Personal Data Processing procedures. All department employees who process Personal Data shall be obligated to follow the instructions of the Data Controller, this Policy and the PDP Procedures.

6.2. Processing of Personal Data without Obtaining Explicit Consent

In circumstances where the Personal Data is stipulated to be Processed without Explicit Consent as per PDP Regulations (LPPD Article 5.2), the Data Controller can process the Personal Data without obtaining the Explicit Consent of the Data Subject. If the Personal Data is processed in this manner, the Data Controller shall Process the Personal Data within the limits determined by the PDP Regulations. In this regard:

(viii) The Personal Data of the Data Subject can be processed by the Data Controller without Explicit Consent, if explicitly allowed by laws.

(ix) Personal Data can be processed by the Data Controller without Explicit Consent to preserve the life or body integrity of a Data Subject who unable to express his/her consent due to physical impossibility or whose consent is not legally recognized as valid and/or another person apart from the Data Subject.

(x) If there is a direct relation with the conclusion, enforcement or execution of an agreement, the Personal Data of the parties to the agreement can be processed by the Data Controller without the Explicit Consent of the Data Subjects.

(xi) If the processing of the Personal Data is mandatory for the Data Controller to fulfill its legal obligations, Personal Data can be processed by the Data Controller without the Explicit Consent of the Data Subjects.

(xii) Personal Data publicized by the Data Subject can be processed by the Data Controller without obtaining Explicit Consent.

(xiii) If the processing of Personal Data is mandatory to establish, use or protect a right, the Personal Data can be processed by the Data Controller without obtaining Explicit Consent.

(xiv) Under the condition of not causing any harm to the fundamental rights and freedoms of the Data Subject, if the Processing of the Personal Data is mandatory for legitimate interest of the Data Controller, Personal Data can be processed by the Data Controller without obtaining Explicit Consent.

VII. PROCESSING OF SENSITIVE PERSONAL DATA

Sensitive Personal Data shall only be processed;

(iii) With the Explicit Consent of the Data Subject; or
(iv) Without the Explicit Consent of the Data Subject,

- Except for sexual life and Personal Health Data, if the processing of the Sensitive Personal Data is explicitly held mandatory as per laws.
- The Personal Data in relation to health and sexual life can only be processed without Explicit Consent by the persons (e.g. Company doctor) or authorized institutes and institutions which are under confidentiality obligation for the purpose of protecting public health, carrying out preventative medicine, medical diagnosis, treatment and care services, planning and management of healthcare services and their financing.

The precautions determined by the Board shall be taken while processing the Sensitive Data. The Data Controller may establish and publish additional policies or procedures with respect to processing of Sensitive Data.

In all circumstances where the Processing of Sensitive Data is necessary, the relevant employee shall inform the Data Controller. In the event it is not clear whether a data is qualified as a Sensitive Data, the relevant department shall refer to the Data Controller.

VIII. TRANSFER OF PERSONAL DATA AND PROCESSING OF PERSONAL DATA BY THIRD PARTIES

The Data Controller may transfer Personal Data to a third party real or legal persons in Turkey and/or abroad, by taking necessary measures in line with the purposes of processing the Personal Data, in accordance with PDP Regulations. In such event, the Data Controller shall ensure that the third parties to whom the Personal Data is transferred adhere to this Policy. In this regard, necessary protective provisions shall be incorporated to the agreements executed with such third party. Each employee shall exhaust the process stipulated under this Policy for Personal Data transfers.

(iii) Transfer of Personal Data to Third Parties in Turkey

Personal Data may be transferred by the Data Controller to third parties in Turkey without obtaining Explicit Consent of the Data subject in exceptional conditions indicated under LPPD Article 5.1 and Article 6.2 or by obtaining Explicit Consent in other conditions set forth under LPPD Article 5.1 and Article 6.2.

Data Controller shall provide that the Personal Data is transferred to the third parties in Turkey in accordance with PDP Regulations.

(iv) Transfer of Personal Data to Third Parties Abroad

Personal Data may be transferred by the Data Controller to third parties abroad without obtaining Explicit Consent of the Data subject in exceptional conditions indicated under LPPD Article 5.2 and Article 6.3 or by obtaining Explicit Consent in other conditions set forth under LPPD Article 5.2 and Article 6.3.

In the event that Personal Data is transferred without obtaining Explicit Consent, in accordance with PDP Regulations, one of the conditions listed below should be met in terms of the foreign country the Personal Data will be transferred to:

- The foreign country which the Personal Data is being transferred to should be amongst the safe countries which have sufficient protection as determined by the Board (please refer to the updated list of the Board), or

- In event that the foreign country which the Personal Data is being transferred to is not in the Board's list of safe countries, the Data Controller and the data controllers in the respective foreign country should apply for permission of the Board with a written undertaking on ensuring the sufficient protection.

Data Controller shall provide that the Personal Data is transferred to the third parties abroad in accordance with PDP Regulations.

IX. OBLIGATION TO INFORM

The Company informs the Data Subject prior to Processing of Personal Data pursuant to the Article 10 of LPPD. In this respect; the Company carries out its Obligation to Inform during the process of obtaining Personal Data. The process of informing Data Subjects within the scope of the Obligation to Inform includes the following: **(i)** Identity of the Data Controller and the representative (if any), **(ii)** The purpose

for processing of Personal Data, **(iii)** To which third parties and for what purposes the processed Personal Data will be transferred, **(iv)** Method of and legal grounds for collecting Personal Data, **(v)** Rights of the Data Subject.

The Company, pursuant to the 20th Article of the Constitution of the Republic of Turkey and the Article 11 of the LPPD, provides the Data Subject the necessary information upon their request.

With regards to ensuring the necessary Obligation to Inform has been fulfilled prior to Processing of Personal Data, Data Controller is jointly liable with the respective employee carrying out the process.

In the event that the Data Processor is a third party other than the Company, the respective third party must undertake to comply with the above-mentioned obligation with a written agreement prior to Processing of Personal Data. Each employee is obliged to follow the process as set forth under this Policy in the event that a third party is transferring Personal Data to the Company.

X. STORAGE, DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Data Controller stores the Personal Data being processed in accordance with LPPD and other legislations in accordance with the periods set forth under the legislation and as long as the legitimate purpose of processing for the Data Controller is still valid in any case.

When the legitimate purpose of processing Personal Data as stipulated by LPPD or other legislation is no longer valid, the relevant Personal Data is either Deleted or Anonymized ex officio or upon the request of Data Subject. In this respect, our Company takes technical and administrative measures required for performance of this obligation. Data Controller may issue and publish additional policies and procedures regarding Deletion and Anonymization of Personal Data.

XI. RIGHTS OF THE DATA SUBJECT

The Company responds to the below requests of Data Subjects whose Personal Data they have possession of in accordance with the PDP Regulations:

- **(ix)** To be informed on whether or not their Personal Data is being processed,
- **(x)** To request information on the processed Personal Data, if processed,
- **(xi)** To be informed on the purpose of processing Personal Data and whether personal data were used as fit for the processing purpose,
- **(xii)** To be informed on the third parties to whom Personal Data were transferred domestically or abroad,
- **(xiii)** To request correction of Personal Data that are incompletely or inaccurately processed by the Company,
- **(xiv)** To request deleting or destroying of the Personal Data which is although processed in accordance with LPPD and other legislative provisions, the grounds for processing Personal Data are no longer valid in terms of purpose, duration and legitimacy,
- **(xv)** To object to occurrence of a result at the detriment of the Data Subject by analyzing the Processed Data exclusively through automated systems,
- **(xvi)** To request compensation of damages in the case that damages are suffered by the Data Subject as a result of unlawful processing of Personal Data,

In the event that Data Subjects wish to exercise their rights listed above, they may either send their request signed with secure electronic signature to the e-mail address of the Data Controller given below which may be changed from time to time or send their requests signed with wet-ink signature to the address of the Data Controller through return receipt courier or notary or submit it by hand along with

documents in proof of the identity of the respective Data Subject, by filling the Application form published on the Company's website.

Data Controller: Konya Hazır Beton Sanayi ve Ticaret Anonim Şirketi
E-mail address: konyahazirbeton@hs03.kep.tr
Address: Horozluhan Mah. Cihan Sok.No:15 Selçuklu/Konya

In the event that Data Subjects submit their requests in relation to their rights listed above in written form to the Data Controller, the Data Controller will conclude their request free of charge within 30 days at utmost, depending on the nature of the request. However, in the event that a fee has been set forth by the Authority, the fee indicated in the tariff determined by the Authority may be requested by the Data Controller.

XII. DATA MANAGEMENT AND SECURITY

All technical and administrative measures to ensure "data security" primarily by prevention of unlawful data processing, prevention of unlawful access to Personal Data and ensuring safe storage of Personal Data as per LPPD Article 12 shall be taken including but not limited to the measures stated below and reserving the further provisions of legislation:

- **(i)** All employees included in the process of protection of Personal Data in accordance with LPPD, this Policy and PDP Procedures shall be severally liable for protection of such data.
- **(ii)** Personal Data Processing operations shall be inspected by the Data Controller with technical systems depending on the technological possibility and application costs.
- **(iii)** For Personal Data Processing operations, personnel with technical know-how are recruited.
- **(iv)** Company employees are informed and trained regarding the protection and legal processing of Personal Data.
- **(v)** Necessary PDP Procedures are issued in the Company to ensure access of the necessary employees to Personal Data.
- **(vi)** Company employees may only access to Personal Data in accordance with the authority that they are given and in compliance with related PDP Procedures.
- **(vii)** Necessary provisions regarding protection of Personal Data is added to the agreements executed with the employees and an awareness is created within the employees in this regard.
- **(viii)** In the event that an employee of the Company is in doubt that Personal Data are duly protected or determines a security gap, he/she shall promptly inform the Data Controller.
- **(ix)** Detailed PDP Procedures on security of Personal Data shall be issued by the Data Controller.
- **(x)** Each person who has been assigned a Company device is responsible for the security of the device they have been assigned for their use.
- **(xi)** Every Company employee or employee working within the Company is responsible for the security of the physical files that are found within their area of responsibility.
- **(xii)** With regards to the additional security measures requested for ensuring security of Personal Data within the scope of PDP Regulations, all employees are obligated to abide by the additional security measures and ensure the sustainability of these security measures.
- **(xiii)** Virus protection systems and firewall software and hardware are set up in line with technological developments for the safe storage of Personal Data in the Company.
- **(xiv)** Back-up programs and sufficient security measures are used to prevent the loss of or damage to Personal Data in the Company.
- **(xv)** If a department within the Company processes Sensitive Personal Data, such department shall be informed by the Data Controller on significance, security and confidentiality of the Personal Data processed by them and such department shall act in compliance with the instructions of the Data Controller. Access authority to Sensitive Personal Data shall only be

given to a limited number of employees. List of such employees shall be prepared and followed by the Data Controller.

(xvi) All Personal Data processed within the Company is deemed by the Company as "Confidential Information."

(xvii) Company employees have been informed that their obligations in relation to the security and confidentiality of Personal Data continues even after termination of the employment relationship and Company employees have undertaken to comply with such rules.

XIII. TRAINING

Data Controller shall give its employees the necessary training on protection of Personal Data in accordance with this Policy, PDP Procedures annexed to it and PDP Regulations.

The trainings shall specifically stress on the definition and practices on protection of Personal Health Data and Sensitive Personal Data.

If an employee has access to Personal Data physically or in computer environment, the Company shall provide training to the respective employee within the scope of this specific access (such as the respective computer software).

XIV. INSPECTIONS

Data Controller has the right to inspect ex officio at all times without giving prior notice that all employees, departments and contactors comply with this Policy and PDP Regulations and shall conduct the necessary routine inspections in this regard.

XV. BREACHES

All employees of the Company shall report to the Data Controller any act, action or work which the employee believes to be in violation of the rules and procedures indicated in the PDP Regulations and this Policy. In this regard, Data Controller shall construct an action plan in accordance with this Policy and PDP Procedures for the respective violation.

Based on the information given to the Data Controller, Data Controller shall to be submitted to Data Subject or the Authority regarding the breach taking into account the current provisions of the legislation.

XVI. OBLIGATIONS

The obligations within the Company shall be vested in -respectively in order -the employee, the department and the Data Controller.

XVII. AMENDMENT OF THE POLICY

This Policy may be amended from time to time with the approval of the Board of Directors of the Company, if required by PDP Regulations or found necessary.

The Company shall share the updated Policy text, in a manner which enables amendments to be reviewed, via e-mail and presents it to Data Subjects via the web address of the Company (www.konyahazirbeton.com.tr).

XVIII. EFFECTIVE DATE OF POLICY

This Policy has been approved by the Company Board of Directors, to be effective as of 7 April 2016.