

BEFA SANAYİ TİC. OTOMOTİV A.Ş

ÖZEL NİTELİKLİ KİŞİSEL VERİLERE İLİŞKİN POLİTİKA

1. POLİTİKANIN AMACI

Bu politikanın amacı; 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'a (Kanun) dayalı olarak çıkarılmış olan ve 30224 sayılı Resmi Gazete'de 28.10.2017 tarihinde yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in (Yönetmelik) 5. ve 6. Maddeleri ve Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Kararı gereği özel nitelikli kişisel verilerin işlenmesine, saklanmasına ve imhasına ilişkin yükümlülüklerin yerine getirilmesi için ŞİRKET genelinde uygulanacak kurallar ile rol ve sorumlulukları belirlemektir.

2. POLİTİKANIN KAPSAMI

Bu Politika kanun hükümleri ile belirlenmiş olan özel nitelikli kişisel verileri işlenen gerçek kişiler ile şirket bünyesinde kişisel verileri işleyen herhangi bir sürece dâhil olan tüm departmanları, çalışanları ve üçüncü tarafları kapsamaktadır. İşbu Politika; Şirket'in özel nitelikli kişisel verileri işleme konusunda uygulayacağı prosedürü ve söz konusu özel nitelikli kişisel verilerin saklanması ve imhasına yönelik kuralları tanımlayacak olup bu alandaki yönetimi sağlayacak tüm faaliyetleri kapsayacaktır.

3. TANIMLAR

Anonim Hale Getirme: Kişisel verilerin başka verilerle eşleştirilse dahi, hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini,

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

Kişisel Veri İşleme Envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,

Kişisel Verileri Koruma Komitesi: Veri sorumlusu tarafından atanmış ve kişisel verilerin korunması kanunu kapsamında oluşturulmuş süreçlerin idari takibi yapan gerçek kişi veya kişileri,

Kişisel Verilerin Silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini,

Kişisel Verilerin Yok Edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemini,

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 verilerini,

Periyodik imha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması

durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini,

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

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

4. POLİTİKA İLE DÜZENLEME ALTINA ALINAN KAYIT ORTAMLARI

Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen özel nitelikli kişisel verilerin bulunduğu her türlü ortam kayıt ortamı kapsamına girer.

Özel nitelikli kişisel veriler elektronik ortamlarda (sunucular, yazılımlar, kişisel bilgisayarlar, mobil cihazlar, çıkartılabilir bellekler) ve elektronik olmayan ortamlarda (kağıt, manuel veri kayıt sistemi, yazılı, basılı, görsel ortamlar) saklanmaktadır.

5.ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

5.1. 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 özel nitelikli kişisel veridir.

5.2. Özel nitelikli kişisel veriler veri sorumlusu tarafından toplanıp işlenecek ise, ilgili kişiden alınacak açık rıza sırasında verinin toplanma ve işlenme sebepleri açık olarak belirtilir.

5.3. Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

5.4. Yukarıda sayılan özel nitelikli kişisel verilerden sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise 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 veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

5.5. Özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

6. BİLGİLENDİRME SÜRECİ (AYDINLATMA YÜKÜMLÜLÜĞÜNÜN KAPSAMI)

Kanunun 10 uncu maddesi gereğince kişisel verilerin elde edilmesi sırasında veri sorumluları veya yetkilendirdiği kişilerce, ilgili kişiler bilgilendirilir. Bu yükümlülük yerine getirilirken veri sorumluları veya yetkilendirdiği kişilerce yapılacak bilgilendirme asgari olarak aşağıdaki konuları içerir:

- Veri sorumlusunun ve varsa temsilcisinin kimliği,
- Kişisel verilerin hangi amaçla işleneceği,
- Kişisel verilerin kimlere ve hangi amaçla aktarılabilceği,
- Kişisel veri toplamanın yöntemi ve hukuki sebebi,
- Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişilerin bildirilmesi,
- Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesi.

7. VERİ TOPLAMA VE AÇIK RIZA ALMA SÜRECİNİN İŞLETİLMESİ

Özel nitelikli kişisel verisi işlenecek olan ilgili kişiden açık rıza alınması kişisel veri temininden önce gerçekleştirilir. İlgiliden alınacak açık rızalar ıslak imzalı olarak ya da elektronik ortamda

alınır. Personel ve aday personelden alınacak açık rızalar için personele taahhütname imzalatılır ve özlük dosyası içerisinde saklanır.

8. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENME ŞARTLARININ ORTADAN KALKMASI DURUMUNDA YAPILACAKLAR

8.1. Şirket, özel nitelikli kişisel veri işleme şartlarının güncelliğinden sorumludur ve bu sorumluluğunu tüm çalışanları ile paylaşır.

8.2. Çalışanlar, veri işleme şartlarının ortadan kalktığı durumlarda veri işlemeye devam edemez. Şirket, şartların ortadan kalktığı ortamları ilgili iş birimlerinin ya da şirket yetkilisinin talebi üzerine işbu politikaya uygun bir şekilde ortadan kaldırmakla yükümlüdür.

8.3. Şirket aşağıda örnek olarak listelenen ve “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik” içinde de belirtilen ilgili durumlarda özel nitelikli kişisel veri işleme şartlarının ortadan kalktığını kabul eder:

- Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,
- Kişisel verileri işlemenin hukuka ve dürüstlük kuralına aykırı olması,
- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması. Veri sorumlusu, kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili gerekli her türlü idari ve teknik tedbirleri almakla yükümlüdür.

8.4. Bu kapsamda Şirket tarafından “Kişisel Veri Saklama ve İmha Politikası” içinde tanımlı olan tedbirler, uygulama esas usulleri ve bu çerçevede alınacak olan aksiyonlar geçerlidir.

9. POLİTİKANIN YÜRÜRLÜĞE SOKULMASI, İHLAL DURUMLARI VE YAPTIRIMLAR

9.1. İşbu Politika tüm çalışanlara duyurularak yürürlüğe girecek ve yürürlüğü itibarıyla tüm iş birimleri, danışmanlar, dış hizmet sağlayıcıları ve sair şirket nezdinde kişisel veri işleyen herkes için bağlayıcı olacaktır.

9.2. Şirket çalışanlarının Politikanın gereklerini yerine getirip getirmediğinin takibi ilgili çalışanların amirlerinin sorumluluğunda olacaktır. Politikaya aykırı davranış tespit edildiğinde konu derhal ilgili çalışanın amiri tarafından bağlı bulunan bir üst amire bildirilecektir. Aykırılığın önemli boyutta olması halinde ise üst amir tarafından vakit kaybetmeksizin şirkete bilgi verilecektir.

9.3. Politikaya aykırı davranan çalışan hakkında, İnsan Kaynakları tarafından yapılacak değerlendirme sonrasında gerekli idari işlem yapılacaktır.

9.4. Politika gereklerinin yerine getirilmesi için şirket tarafından; gerekli tüm güvenlik önlemleri alınmaktadır.

10. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALACAK KİŞİLER VE SORUMLULUKLARI

Şirket içerisinde Kanun, Yönetmelik ve Politika ile belirtilen verinin imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar ve sair surette şirket nezdinde kişisel veri saklayan ve işleyen herkes bu gerekleri yerine getirmekten sorumludur.

Her iş birimi kendi iş süreçlerinde ürettiği veriyi saklamak ve korumakla yükümlüdür; ancak üretilen verinin iş biriminin kontrolü ve yetkisi dışında sadece bilgi sistemlerinde bulunması durumunda, söz konusu veri bilgi sistemlerinden sorumlu birimler tarafından saklanacaktır.

İş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar doğmasına neden olacak periyodik imhalar, ilgili kişisel verinin türü, içinde yer

aldığı sistemler ve veri sahibi iş birimi dikkate alınarak ilgili bilgi sistemleri bölümlerince yapılacaktır.

Özel Nitelikli kişisel verilerin saklama ve imha süreçlerinde yer alacak kişiler ve sorumlulukları şu şekildedir;

UNVAN	BİRİM	GÖREV
Şirket Yetkilisi	Şirketi Yönetimi	Çalışanların politikaya uygun hareket etmesinden sorumludur.
Şirket Yetkilisi	Şirket Yönetimi	Politikanın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
İdari İşler, Muhasebe, Pazarlama/Satış	Diğer Birimler	Görevlerine uygun olarak politikanın yürütülmesinden sorumludur.

11. TEKNİK VE İDARİ TEDBİRLER

Şirket tarafından özel nitelikli kişisel verilerin, hukuka aykırı olarak işlenmesini ve erişilmesini önlemek ve muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirler alınır; Kanun hükümlerinin ve Kurul Kararı'nın uygulanmasını sağlamak amacıyla gerekli denetimlerin yapılması sağlanır.

11.1. Teknik Tedbirler

- Kişisel veri içeren bilgi teknoloji sistemlerinin ve verilerin korunması amacıyla, antivirüs ve güvenlik duvarı yazılım ve donanımları kullanılır.
- Kullanılmayan yazılım ve servislerin cihazlardan silinmesi sağlanır.
- Yazılım ve donanımların düzgün bir şekilde çalışması, alınan güvenlik önlemlerinin yeterli olup olmadığı ve verilerin bulunduğu ortamlara ait güvenlik güncellemeleri düzenli olarak kontrol edilir. Gerekli güvenlik testleri düzenli olarak yapılarak test sonuçları kayıt altına alınır. Olası güvenlik açıklarının kapatılması için gerekli yama ve yazılım güncellemelerinin yapılması sağlanır.
- Özel nitelikli kişisel veri içeren sistemlere erişim, erişim politikaları, kullanıcı ve rol yönetimi prosedürleri çerçevesinde sağlanır. Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamı ve süreleri net olarak tanımlanır.
- Verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sistemi kullanılır.
- Periyodik olarak yetki kontrolleri gerçekleştirilir.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri derhal kaldırılır. Bu kapsamda, Şirket tarafından kendisine tahsis edilen envanter iade alınır.
- Verilerin kurum dışına sızmasını engelleyecek veya gözlemleyecek teknik altyapının temin edilmesi sağlanır.
- Özel nitelikli kişisel verilerin bulunduğu ortamın niteliğine göre yeterli güvenlik önlemleri (elektrik kaçağı, yangın, su baskını, hırsızlık vb. durumlara karşı) alınır. Bu ortamların fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenir.

- Özel nitelikli kişisel verilerin güvenli bir biçimde saklanmasını sağlamak için verilerin yedeklenmesi ve tüm yedeklerin fiziksel güvenliği sağlanır.
- Özel nitelikli kişisel verilerin geri dönüştürülemez ve denetim izi bırakmayacak şekilde yok edilmesi sağlanır.
- Bulut ortamında yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması; bulut bilişim hizmet ilişkisi sona erdiğinde ise; kişisel verileri kullanılabilir hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi sağlanır.
- Özel nitelikli kişisel verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya Kayıtlı Elektronik Posta (KEP) hesabı kullanılarak aktarılması sağlanır.

11.2. İdari Tedbirler

- Özel nitelikli kişisel verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığının ve gerçekleşmesi durumunda yol açacağı kayıpların belirlenerek, risklerin azaltılması veya ortadan kaldırılmasına yönelik tedbirlerin alınması sağlanır.
- Özel nitelikli kişisel verilerin işlenmesi, gizliliğinin ve güvenliğinin sağlanması ve imha edilmesine ilişkin tüm politika ve prosedürler ile ilgili süreçlerde görev alan personelin görev, yetki ve sorumlulukları yazılı hale getirilir ve tüm personelin erişimine sunulur.
- Personele Kanun ve buna bağlı yönetmelikler ile özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi sağlanır.
- Politika ve prosedürlerin güncel tutulması ve yapılan değişikliklerle ilgili çalışanlara gerekli eğitimlerin verilmesi ve bilgilendirmeler yapılması sağlanır.
- İşe alım süreci kapsamında, çalışanlar ile Şirket arasında düzenlenen sözleşmelerle özel nitelikli kişisel verilerin korunması ve gizliliğinin sağlanmasına ilişkin hükümler eklenip çalışan tarafından imzalanması sağlanır.
- İşlenen kişisel verilere hala ihtiyaç olup olmadığı ve doğru yerde muhafaza edilip edilmediği tespit edilerek, arşiv amaçlı tutulan kişisel verilerin, daha güvenli ortamlarda muhafaza edilmesi, ihtiyaç duyulmayan özel nitelikli kişisel verilerin ise işbu politika doğrultusunda silinmesi, yok edilmesi veya anonim hale getirilmesi sağlanır.
- Saklanan kişisel verilere Şirket içi erişim, görev tanımı gereği erişmesi gerekli personel ile sınırlandırılır.
- Çalışanların Şirket tarafından belirlenip duyurulan politika ve prosedürlerine uymaması durumunda Disiplin Prosedürü doğrultusunda yaptırımlar uygulanır.
- Özel nitelikli kişisel verilerin paylaşılması ile ilgili olarak, Özel nitelikli kişisel verilerin paylaşıldığı kişiler ve veri işleyenler ile özel nitelikli kişisel verilerin korunması ve veri güvenliğine ilişkin gizlilik sözleşmeleri imzalanır veya mevcut sözleşmelere veri güvenliğine ilişkin hükümler eklenir.
- Politika ve prosedürler kapsamında; düzenli olarak kontroller yapılır, gelişime açık alanlar için

gerekli aksiyonlar planlanıp uygulamaya alınır.

- Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimlerin yapılması ve denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetleri için aksiyonlar planlanarak bulguların derhal giderilmesi sağlanır.

- İşlenen özel nitelikli kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durum en kısa sürede ilgisine ve Kurul'a bildirilir.

12. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VEYA ANONİM HALE GETİRİLMESİ

Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.

Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanun'un 4. maddesindeki genel ilkeler ile 11. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve Kişisel Veri Saklama ve İmha Politikası'na uygun hareket edilmektedir.

13. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

Özel Kişisel Verileri Saklama ve İmha Süreleri Kişisel Veri İşleme Envanterinde yer almaktadır. Periyodik imha ya da talep üzerine gerçekleştirilecek imha işlemlerinde söz konusu saklama ve imha süreleri dikkate alınacaktır.

İşlenen kişisel verilerin saklanması için mevzuatta öngörülen süreler var ise bu veriler mevzuatta öngörülen süre kadar saklanmak zorundadır. Bu verilere ilişkin imha işlemi ancak mevzuatta öngörülen sürelerin dolmasının ardından yapılabilir. Özel nitelikli kişisel verileri saklama ve imha süreleri şu şekildedir;

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
İdari İşlerin Yürütülmesi	İş Akdinin Sona Ermesinden İtibaren 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresi
Muhasebe	İş Akdinin Sona Ermesinden İtibaren 10 Yıl	Saklama Süresinin Bitimini Takip Eden İlk Periyodik İmha Süresi

14. PERİYODİK İMHA SÜRELERİ

Özel Nitelikli Kişisel Verileri Periyodik İmha Süresi veri sahibi ilgili iş birimleri tarafından tespit ve tayin edilir; ancak her hâlükârda bu süre 6 (altı ayı) ayı geçemez. Buna göre, Kurumda her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

15. YÜRÜRLÜK

Politika yayımlanma tarihi itibari ile yürürlüğe girecektir.