BERKO KİŞİSEL VERİLERİ SAKLAMA VE İMHA POLİTİKASI

1. AMACI

Bu politikanın amacı; "*Kişisel Verilerin Korunması Hakkında Kanun*" ve "*Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik*"'in gereği kişisel verilerin saklanması ve imhasına ilişkin yükümlülüklerin ve Yönetmelik'te belirtilen sair yükümlülüklerin yerine getirilmesi için Berko İlaç ve Kimya San.A.Ş.(Şirket) genelinde uygulanacak kurallar ile rol ve sorumlulukları belirlemektir.

2. KAPSAMI

Politika, Şirket nezdinde tutulan, Kanun ile tanımlanan kişisel verileri ve özel nitelikli kişisel verileri, tüm Şirket çalışanlarını, yöneticilerini, danışmanlarını ve kişisel veri paylaşımı söz konusu olan tüm durumlarda iştiraklerini, dış hizmeti sağlayıcılarını ve Şirket'in sair hukuki ilişkiye girdiği gerçek ve tüzel kişileri kapsamaktadır. Politika Kanun'da belirtildiği şekilde, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla verilerin işlendiği sistemlerde yer alan kişisel verileri kapsamaktadır. Politikada aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel veriler birlikte "Kişisel Veriler" olarak adlandırılacaktır.

3.TANIMLAR

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

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,

Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan yazılı beyan,

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

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,

Maskeleme: Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin silinmesi, boyanması ve yıldızlanması gibi işlemleri,

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

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,

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

Periyodik imha: Kanunda yer alan kişisel verilerin işlenme 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,

Kişisel Veri Saklama Tablosu: Kişisel verilerin Şirket nezdinde tutulacağı süreleri gösteren tabloyu,

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 kişisel verilerin bulunduğu her türlü ortam kayıt ortamı kapsamına girer.

Veri sahiplerine ait kişisel veriler, Şirket tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır:

Elektronik ortamlar:

- EXCHANGE SERVER
- SAP – SUCCESS FACTORS
- FİLE SERVER
- VERİBASE
- POLİMEK-PDKS
- DAPHNE
- MDM
- GÜVENLİK KAMERA
- DC DHCP
- DC
- DC 2

Fiziksel ortamlar:

- Birim Dolapları
- Arşiv

5. KİŞİSEL VERİLERİ KORUMA BİRİMİ'NİN GÖREV VE YETKİLERİ

5.1. Kişisel Verileri Koruma Birimi Politikanın ilgili iş birimlerine duyurulmasından ve gereklerinin Şirket birimlerince yerine getirilmesinin takibinden sorumludur.

5.2. Kişisel Verileri Koruma Birimi kişisel verilerin korunmasına ilişkin mevzuat değişiklikleri, Kurulun düzenleyici işlemleri ile kararları, mahkeme kararları veya süreç, uygulama ve sistemlerdeki değişiklikler gibi durumları ilgili iş birimlerinin takip etmesi ve gerekiyorsa iş süreçlerini güncellemeleri için gerekli duyuruları ve bildirimleri yapar,

5.3. Kişisel Verileri Koruma Birimi; Kanun ve ikincil düzenlemeleri ile Kurulun kararları ve düzenlemeleri, mahkeme kararları ve sair yetkili makamların kararlarının ve/veya taleplerinin incelenmesi, değerlendirilmesi, takibi ve sonuçlandırılmasına yönelik süreçleri belirler ve ilgili birimlere duyurur.

6.KİŞİSEL VERİLERİN SAKLANMASIYLA İLGİLİ TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesinin, erişilmesinin önlenmesi ve verilerin hukuka uygun olarak imha edilmesi amacıyla KVKK'nm 12. maddesindeki ilkeler çerçevesinde, Şirket tarafından alınmış olan tüm idari ve teknik tedbirler aşağıda sayılmıştır:

6.1. İdari Tedbirler:

6.1.1. Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
6.1.2.İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.
6.1.3. Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar.
6.1.4. Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.
6.1.5. Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.

6.2. Teknik Tedbirler:

6.2.1. Kurulan sistemler kapsamında gerekli iç kontrolleri yapar.
6.2.2. Kurulan sistemler kapsamında bilgi teknolojileri risk değerlendirmesi ve iş etki analizinin gerçekleştirilmesi süreçlerini yürütür.
6.2.3. Verilerin kurum dışına sızmasını engelleyecek veyahut gözlemleyecek teknik altyapının temin edilmesini ve ilgili matrislerin oluşturulmasını sağlar.
6.2.4.Düzenli olarak ve ihtiyaç oluştuğunda sızma testi hizmeti alarak sistem zafiyetlerinin kontrolünü sağlar.
6.2.5. Bilgi teknolojileri birimlerinde çalışanların kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlar.
6.2.6. Kişisel verilerin yok edilmesi geri dönüştürülemeyecek ve denetim izi bırakmayacak şekilde sağlanır.
6.2.7. Kanun'un 12. maddesi uyarınca, kişisel verilerin saklandığı her türlü dijital ortam, bilgi güvenliği gereksinimlerini sağlayacak şekilde şifreli veyahut kriptografik yöntemler ile korunur.

7. KİŞİSEL VERİLERİN İŞLENME ŞARTLARININ ORTADAN KALKMASI DURUMUNDA YAPILACAKLAR

7.1. Kişisel verilerin işlenmesine yönelik amaç unsurunun ortadan kalkması, açık rızanın geri alınmış olması veya Kanunun 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması ya da adı geçen maddelerde istisnalardan hiçbirinin uygulanamayacağı bir durumun söz konusu olması halinde, işlenme şartları ortadan kalkan kişisel veriler, ilgili iş birimi tarafından, iş ihtiyaçları göz önüne alınarak, Yönetmeliğin 7., 8., 9. veya 10. maddeleri kapsamında, uygulanan yöntemin gerekçesi de açıklanmak suretiyle maskelenir, silinir, yok edilir veya anonim hale getirilir.

Ancak kesinleşmiş bir mahkeme kararının söz konusu olması halinde mahkeme kararı ile hükmedilen imha yöntemi uygulanmak zorundadır.

7.2. Kişisel veriyi işleyen ya da saklayan tüm kullanıcılar ve veri sahibi Şirket birimleri işlemeyle ilgili şartların ortadan kalkıp kalkmadığını en geç 6 aylık periyotlar içerisinde, kullandıkları veri kayıt ortamlarında gözden geçireceklerdir. Kişisel veri sahibinin başvurusu ya da Kurulun veya bir mahkemenin bildirimi üzerine, ilgili kullanıcı ve birimler, periyodik denetleme süresine bakmaksızın kullandıkları veri kayıt ortamlarında bu gözden geçirmeyi yapacaklardır.

7.3. Periyodik gözden geçirmeler neticesinde veya herhangi bir anda veri işleme şartlarının ortadan kalkmış olduğu tespit edildiğinde ilgili kullanıcı veya veri sahibi, ilgili kişisel verinin kendi uhdesinde bulunan kayıt ortamından işbu politikaya göre silinmesine, yok edilmesine veya anonim hale getirilmesine karar verecektir. Tereddüt duyulan durumlarda ilgili veri sahibi iş biriminden görüş alınarak işlem yapılacaktır. Merkezi Bilgi Sistemlerinde yer alan çok paydaşlı veri sahipliği bulunan kişisel verilerin imhasına yönelik karar alınması gerektiğinde ise Kişisel Verileri Koruma Birimi'nin görüşü alınacak ve söz konusu kişisel veri hakkında işbu politikaya göre verinin saklanmasına veya silinmesine, yok edilmesine veya anonim hale getirilmesine ilgili veri sahibi iş birimi tarafından karar verilecektir.

7.4. Kişisel verilerin maskelenmesi, silinmesi, yok edilmesi veya anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süreyle saklanır.

7.5. Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde Kanunun 4. maddesindeki genel ilkeler ile 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve mahkeme kararlarına uygun hareket edilmesi zorunludur.

7.6. Bir kişisel verinin sahibi gerçek kişi, Kanunun 13. maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini, yok edilmesini veya anonim hale getirilmesini talep ettiğinde, ilgili veri sahibi iş birimi, kişisel verileri işleme şartlarının tamamının ortadan kalkıp kalkmadığını inceler. İşleme şartlarının tamamı ortadan kalkmışsa; talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Talep, başvuru tarihinden itibaren en geç 30 gün içinde sonuçlandırılır ve ilgili kişiye Kişisel Verileri Koruma Birimi aracılığıyla bilgi verilir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu kişisel veriler üçüncü kişilere aktarılmışsa, ilgili veri sahibi iş birimi bu durumu derhal aktarım yapılan üçüncü kişiye bildirir ve üçüncü kişi nezdinde Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder.

7.7. Kişisel verileri işleme şartlarının tamamının ortadan kalkmadığı durumlarda, kişisel veri sahiplerinin verilerinin silinmesi veya yok edilmesine yönelik talepleri Şirket tarafından Kanunun 13. maddesinin 3. fıkrası uyarınca gerekçesi açıklanarak reddedilebilir. Ret cevabı ilgili kişiye en geç 30 gün içerisinde yazılı olarak ya da elektronik ortamda bildirilir.

7.8. Kişisel verilerin silinmesi ya da yok edilmesine yönelik talepler ancak ilgili kişinin kimlik tespitinin yapılmış olması kaydıyla değerlendirilecektir. Söz konusu kanallar dışında yapılacak taleplerde ilgili kişiler kimlik tespitinin ya da doğrulamasının yapılabileceği kanallara yönlendirilecektir.

8. POLİTİKANIN YÜRÜRLÜĞE SOKULMASI, İHLAL DURUMLARI VE YAPTIRIMLAR

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

8.2. Şirket çalışanlarının Politikanın gereklerini yerine getirip getirmediğinin takibi ilgili çalışanların üstlerinin sorumluluğunda olacaktır. Politikaya aykırı davranış tespit edildiğinde, konu derhal, ilgili çalışanın üstü tarafından, bağlı bulunan müdüre bildirilecektir. Aykırılığın önemli boyutta olması halinde ise, müdür tarafından vakit kaybetmeksizin Kişisel Verileri Koruma Birimi'ne bilgi verilecektir.

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

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

Genel olarak Şirket içerisinde Kanun, Yönetmelik ve Politika ile belirtilen verinin imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar, danışmanlar, dış hizmet sağlayıcıları ve sair surette Şirket nezdinde kişisel veri saklayan ve işleyen herkes, bu gerekleri yerine getirmekten sorumludur. Özel olarak görevlendirilen personelin unvan, birim ve görev listesi Tablo Ek:1'de yer almaktadır. 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.

10. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo Ek: 2'de yer almaktadır. Periyodik imha ya da talep üzerine gerçekleştirilecek imha işlemlerinde söz konusu saklama ve imha süreleri dikkate alınacaktır. Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo Şirket kişisel veri envanterinde yer alacak süreçlerin sahibi iş birimlerince, tereddüt halinde Kişisel Verileri Koruma Birimi değerlendirmeleri de alınarak, güncellenecektir.

11. PERİYODİK İMHA SÜRELERİ

Kişisel Verileri Periyodik İmha Süresi veri sahibi ilgili iş birimleri tarafından tespit ve tayin edilir; ancak her hâlükârda bu süre 6 (altı) ayı geçemez.

12. KİŞİSEL VERİLERİN SİLİNMESİ, YOK EDİLMESİ VE ANONİMLEŞTİRİLMESİ TEKNİKLERİ

12.1 Kişisel Verilerin Silinmesi:

Yazılımdan Güvenli Olarak Silme: Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken; İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır. Bulut sisteminde ilgili verilerin silme komutu verilerek silinmesi; merkezi sunucuda bulunan dosya veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması; veri tabanlarında ilgili satırların veri tabanı komutları ile silinmesi; taşınabilir medyada yani flash ortamında bulunan verilerin uygun yazılımlar kullanılarak silinmesi bu kapsamda sayılabilecektir.

Ancak, kişisel verilerin silinmesi işlemi, diğer verilere de sistem içerisinde erişilememe ve bu verileri kullanamama sonucunu doğuracak ise, aşağıdaki koşulların sağlanması kaydıyla, kişisel verilerin ilgili kişiyle ilişkilendirilemeyecek duruma getirilerek arşivlenmesi halinde de kişisel veriler silinmiş sayılacaktır.

– Başka herhangi bir kurum, kuruluş veyahut kişinin erişimine kapalı olması,
– Kişisel verilere yalnızca yetkili kişiler tarafından erişilmesini sağlayacak şekilde gerekli her türlü teknik ve idari tedbirlerin alınması.

Uzman Tarafından Güvenli Olarak Silme: Bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilecek biçimde güvenli olarak silinir.

Kağıt Ortamında Bulunan Kişisel Verilerin Karartılması(Maskeleme): Kişisel verilerin amaca yönelik olmayan kullanımını önlemek veya silinmesi talep edilen verileri silmek için, ilgili kişisel verilerin fiziksel olarak kesilerek belgeden çıkartılması veya geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünemeyecek hale getirilmesi, kapatılması yöntemidir.

12.2.Kişisel Verilerin Yok Edilmesi:

12.2.1 Elektronik Kayıtlar;
Fiziksel Yok Etme,
Üzerine Yazma ve yollarıyla yok edilebilir.
Kişisel verilerin yer aldığı flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları için, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.
CD, DVD gibi veri saklama ortamlarında yer alan kişisel veriler, yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilir.
Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimlerinde yer alan kişisel veriler, tüm veri kayıt ortamlarının söküldüğü doğrulandıktan sonra birimin niteliğine göre uygun yok etme yöntemi seçilir.

12.2.2 Fiziksel Kayıtlar ise kağıt imha veya kırpma makineleri ile anlaşılmaz boyutta (mümkünse dikey ve yatay şekilde parçalanarak) veya okunmasını imkânsız kılacak başka yöntemlerle (örneğin, Kayıt'ı birleştirilemeyecek ufak parçalara kesmek veya fiziksel kaydı uygun bir ortamda yakmak vb.) imha edilir.

12.2.3 Bulut sistemleri için; bu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenir ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılır. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir.

12.2.4 Arızalanan ya da bakıma gönderilen cihazlar için; bu cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

a) İlgili cihazların bakım, onarım işlemi için üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin uygun yöntemle yok edilmesi

b) Yok Etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,

c) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması,

12.3.Kişisel Verilerin Anonim Hale Getirilmesi Teknikleri:

12.3.1.Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri,

Saklanmakta olan kişisel verilerde bir değişiklik veya ekleme/çıkarma yapılmaksızın; herhangi bir kişisel veri grubunun genelleme, birbiri ile yer değiştirme veya gruptan belirli bir veri veya alt veri grubunun çıkarılması ile uygulanan anonimleştirmeye yöntemleridir.

Değişken Çıkartma: Betimleyici nitelikteki verilerin çıkartılması yöntemi ile toplanılan verilerin bir araya getirilmesinden sonra oluşturulan veri setindeki değişkenlerden "yüksek dereceli betimleyici" olanlar çıkarılarak mevcut veri seti anonim hale getirilmektedir

Kayıtları Çıkartma: Kayıttan çıkarma yönteminde veriler arasında tekillik ihtiva eden veri satırı kayıtlar arasından çıkaralar saklanan veriler anonim hale getirilmektedir. Örneğin, bir şirkette tek kıdemli müdür var ise bu kişiye ait verilerin birbirleri ile aynı kademede bulunan çalışanların kıdem, maaş ve cinsiyet verilerinin tutulduğu kayıtlardan çıkarılması ile kalan veriler anonim hale getirilebilecektir.

Bölgesel Gizleme: Bölgesel gizleme yönteminde ise tek bir verinin çok az görülebilir bir kombinasyon yaratması sebebi ile belirleyici niteliği mevcut ise ilgili verinin gizlenmesi anonimleştirmeyi sağlamaktadır. Örneğin, şirketin futbol takımının yedek listesinde olan ilgili veri sorumluları arasında yalnızca bir kişi 65 yaşında ise yaş, cinsiyet ve sağlık durumu yönünden futbol oynayabilecek olup olmadığı bilgisinin birlikte saklandığı bir veri kümesinde 'Yaş:65' yerine 'Bilinmiyor' yazılması veya bu kısmın boş bırakılması anonimleştirmeyi sağlayacaktır.

Alt ve Üst Sınır Kodlama: Alt ve üst sınır kodlaması yöntemi ile önceden tanımlanmış kategorilerin yer aldığı bir veri grubundaki değerlerin belirli bir ölçüt belirlenerek birleştirilmesiyle anonim hale getirilmektedir.

Genelleştirme: Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örneğin; çalışanların yaşlarının tek tek göstermeksizin X yaşında Z kadar çalışan bulunduğunun ortaya konulması.

Global Kodlama: Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örneğin; doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen bölgenin belirtilmesi.

12.3.2.Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

Değer düzensizliği sağlayan anonim hale getirme yöntemlerinde değer düzensizliği sağlamayanların aksine kişisel veri gruplarında bazı verilerin değiştirilmesi ile bozulma yaratmaktadır. Bu yöntemler kullanılırken elde edilmesi beklenen/istenen fayda doğrultusunda sapmaların dikkatli uygulanması gerekecektir. Toplam istatistiklerin bozulmaması sağlanarak veriden beklenen fayda sağlanmaya devam edilebilir.

Gürültü Ekleme: Verilere gürültü ekleme yöntemi özellikle sayısal verilerin ağırlıklı olduğu bir veri setinde mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eklenerek veriler anonim hale getirilmektedir. Örneğin, kilo değerlerinin olduğu bir veri grubunda (+/−) 3 kg sapması kullanılarak gerçek değerlerin görüntülenmesi engellenmiş ve veriler anonimleştirilmiş olur. Sapma her değere eşit ölçüde uygulanır.

Birleştirme: Mikro birleştirme yönteminde tüm veriler ilk olarak anlamlı bir sıraya dizilerek (büyükten küçüğe gibi) gruplara ayrılıp, grupların ortalaması alınarak elde edilen değer mevcut gruptaki ilgili verilerin yerine yazılarak anonimleştirme sağlanmış olacaktır. Örneğin, maaş bilgisi için; 10.000 TL altı ve üstü iki grup yapılır ise, 10.000 ve daha az maaş alan kişilerin maaşlarının toplamı kişi sayısına bölünür ve 10.000TL altında maaş alan herkesin maaş kümesine elde edilen bu değer yazılır.

Veri Değiş Tokuşu: Veri değiş tokuşu yönteminde saklanan veriler içerisinden seçilen çiftler arasında bir değişkenin değerleri birbiri ile değiştirilir. Genel olarak kategorize edilebilen veriler için kullanılan bu yöntemde amaç veri sahiplerine ait verilerin birbirleri ile değiştirilerek veri tabanının dönüştürülmesidir.
Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler şirketimizce kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3(üç) yıl süreyle saklanır.

12. YÜRÜRLÜK

12.1. Politika yayınlanma tarihi itibari ile yürürlüğe girecektir.

12.2. Politikanın Şirket genelinde duyurulması ve gerekli güncellemelerin yapılması Kişisel Verileri Koruma Birimi'nin sorumluluğundadır.

EKLER: 1- Personel Unvan, Birim Ve Görev Listesi
2- Saklama Ve İmha Süreleri Tablosu

Yayın Tarihi : 10.07.2018
Versiyon : 2

EK-1
PERSONEL UNVAN, BİRİM VE GÖREV LİSTESİ

PERSONEL	GÖREV	SORUMLULUK
ARGE Koordinatörü Serap Odabaşı	Araştırma Geliştirme Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetim
Bilgi İşlem Müdürü Erol Karaca	Bilgi Teknolojileri Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetim
Dış Pazarlar Proje Müdürü S.Aykut Adalmaz	Dış Ticaret Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetim
Fabrika Müdürü Nursel Gülsoy	Fabrika Genel- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Hukuk Müşaviri Şükrü Aymelek	Sözleşmeler - Kişisel veri saklama ve imha politikası uygulama ana sorumlusu-**Veri Sorumlusu Temsilcisi**	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetim ve düzenli denetimlerin yapılması
İdari İşler Şefi H.Medeni Yılmaz	İdari İşler Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetim
İnsan Kaynakları Müdürü İbrahim Sariyar	İnsan Kaynakları Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Kalite Güvence ve Mesul Müdür Haluk Akkuş	Kalite Güvence Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Kalite Kontrol Müdürü Erol Taşkan	Kalite Kontrol Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Kurumsal İletişim Şefi Fidan Akur	Kurumsal İletişim Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Mali İşler Müdürü	Mali İşler Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile

Cem Günbay		periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Grup Ürün Müdürü Savaş Duman	Pazarlama Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Ruhsatlandırma Müdürü Neslihan Esen	Ruhsatlandırma ve Farmakovijilans Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Satın Alma Esin Aksu	Satın Alma Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Satış Koordinatörü Hüseyin Polat	Satış Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Satış Muhasebe Selçuk Uğur	Satış Muhasebe Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Üretim Müdürü Ersin Hayran	Üretim Planlama Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Üretim Planlama Müdürü Elif Öztürk	Üretim Planlama Departmanı- Kişisel veri saklama ve imha politikası uygulama sorumlusu	Görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi

EK-2
SAKLAMA VE İMHA SÜRELERİ TABLOSU

Kişisel veriler aksine bir kesinleşmiş mahkeme kararı veya ihtiyati tedbir kararı bulunmadıkça Politikanın 7. maddesinde belirtilen hususlar dikkate alınarak aşağıdaki tabloda belirtilen süreler boyunca saklanacak, süre sonunda ise imha edilecektir:

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
Bakanlıklar/Kamu Kurumları/İhale dökümanları	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel ile ilgili mahkeme / icra bilgi taleplerinin cevaplanması	İş ilişkisi bitim sonrası 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Üçüncü kişilerle imzalanan sözleşmeler	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel özlük dosyası	İş ilişkisi bitim sonrası 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Olumsuz sonuçlanan iş başvuruları	Başvurunun olumsuz sonuçlanmasından itibaren 2 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Ücret ve maaşa ilişkin tüm dökümanlar	İş ilişkisi bitim sonrası 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel özel sağlık ve ferdi kaza sigorta poliçeleri	İş ilişkisi bitim sonrası 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Taşıt plaka bilgileri (üçüncü kişiler)	Kaydedildiği tarihten itibaren 1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İş sağlığı ve güvenliği uygulamaları	İş ilişkisi bitim sonrası 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Kayıt/Takip/Log Sistemleri	1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Güvenlik kamera görüntüleri	Görüntünün alındığı tarihten itibaren 3 ay	Saklama süresinin bitimini takiben 90 gün içerisinde
Ödeme işlemleri	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Personel Finansman Süreçleri	İş ilişkisi bitim sonrası 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Sözleşme sürecinin kişisel verilerle ilgili bölümü ve sözleşmenin muhafazası	İş ilişkisi bitim sonrası 10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
İnternet ve wifi aracılığı ile elde edilen bilgiler	Kayıt tarihinden itibaren 1 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Talep / Şikayet Bilgileri	Kaydın alınmasından itibaren 5 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Her türlü doküman dosyalanması	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde

Eğitim kayıtlarının dosyalanması	10 yıl	Saklama süresinin bitimini takiben 180 gün içerisinde
Kişisel verinin TCK veya sair ceza hükmü getiren mevzuat kapsamında bir suça konu olması veya bir suç ile ilişkili olması durumunda TCK'nun 66. ve 68. maddeleri gereği	Dava zamanaşımı ve Ceza Zamanaşımı müddetince	