EagleBurgmann
a member of EKK and FREUDENBERG

RELY ON EXCELLENCE

İNTERNET SİTESİ İLETİŞİM FORMU DOLDURAN KİŞİLER HAKKINDA KİŞİSEL VERİLERİN KORUNMASI AYDINLATMA VE BİLGİLENDİRMESİ

1. Bu internet sitesine giren kişiler elektronik formu doldurmak suretiyle kişisel verilerinin kişisel verilerinin aşağıda açıklanan amaçlar doğrultusunda kaydedilmesi, işlenmesi, aktarılması, silinmesi, yok edilmesi ve anonimleştirilmesi hakkında veri sorumlusu sıfatıyla **Eagle Burgmann End. Sız. San. ve Tic. Ltd. Sti.** Şirketi tarafından aydınlatılmaktadır.

2. İşbu bilgilendirme 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun 10.maddesinde düzenlenen Veri sorumlusunun aydınlatma yükümlülüğü hükümleri kapsamında yapılmaktadır.

3. **Kişisel Verilerinizin İşlenmesi** - Aşağıda başlıkları belirtilen kişisel verilerinizi kişisel veri envanterine kişisel veriler politikamızda belirtilen şekillerde kaydedilmektedir.

- **3.1.** Ad
- **3.2.** Soyad
- **3.3.** E-posta adresi
- **3.4.** Ülke bilgisi
- **3.5.** Çalıştığı şirket bilgisi
- **3.6.** IP Adresi
- **3.7.** Formda paylaştığınız mesajınız
- **3.8.** Tarayıcı bilgileri

4. **Kişisel Verilerinizin Toplama Yöntemi :** Kişisel verileriniz https://www.eagleburgmann.com İnternet sitesinde yazılımlar aracılığıyla elde edildikten sonra yönlendirilen iletişim formuna girdiğiniz kişisel verileri veri tabanına işleyen yazılımı aracılığıyla kaydedilmektedir.

5. **Kişisel Veri İşleme Amaçları:** Bu kapsamda, kişisel verileriniz aşağıdaki amaçlar doğrultusunda özel veritabanı yazılımlar aracılığıyla işlenmektedir.

- **5.1.** Bilgi Güvenliği Süreçlerinin Yürütülmesi
- **5.2.** Faaliyetlerin Mevzuata Uygun Yürütülmesi
- **5.3.** İş Faaliyetlerinin Yürütülmesi / Denetimi
- **5.4.** İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi
- **5.5.** İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
- **5.6.** Saklama Ve Arşiv Faaliyetlerinin Yürütülmesi
- **5.7.** Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
- **5.8.** Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
- **5.9.** Şirket'in ana faaliyet konusundaki hizmetleri yönetilmesi ve yürütülmesi,
- **5.10.** Şirket'in sözleşmesel yükümlülüklerinin yerine getirilmesi,
- **5.11.** Verilerin analiz edilerek şirket ve internet sitesindeki hizmetlerin geliştirilmesi
- **5.12.** İletişim formunu dolduran kişilere daha hızlı ve etkin bir şekilde hizmet verilmesi

6. **Kişisel Verilerinizin İşlenmesinin Hukuki Sebepleri:** Kişisel Verileriniz aşağıdaki hukuki sebeplerle işlenmektedir:

- **6.1.** Kanunlarda öngörülmesi
- **6.2.** Sözleşme imzalanması
- **6.3.** Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması
- **6.4.** İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması

7. **Kişisel verilerinizin aktarılması**, Şirket ziyaret kaydınızla ilişkin kişisel veriler aşağıdaki kişi ve kuruluşlara aktarılabilecektir.

7.1. Gerçek Kişiler Ve Özel Hukuk Tüzel Kişileri

7.2. Hissedarlar

7.3. İş Ortağı

7.4. İştirak Ve Bağlı Ortaklıklar

7.5. Tedarikçi

7.6. Topluluk Şirketi

7.7. Yetkili Kamu Kurum Ve Kuruluşları

8. **Haklarınız** - Şirket tarafından verilerinizin işlendiği ve Şirket'in verilerinizi veri sorumlusu sıfatı ile işlediği ölçüde kişisel verileriniz bakımından aşağıda bulunan haklara sahipsiniz:

8.1. Herhangi bir kişisel verinizin işlenip işlenmediğini öğrenme;

8.2. Kişisel verilerinizin işlenme faaliyetlerine ilişkin olarak bilgi talep etme;

8.3. Kişisel verilerinizin işlenme amaçlarını öğrenme;

8.4. Kişisel verilerin yurt içinde veya yurt dışında üçüncü kişilere aktarılmış olması durumunda bu kişileri öğrenme;

8.5. Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme;

8.6. Kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması veya Şirket'in söz konusu verileri işleyebilmek için hukuki dayanağı veya meşru menfaatinin bulunmaması halinde kişisel verilerin silinmesini veya yok edilmesini isteme;

8.7. Şirket'ten, yine Şirket tarafından yetkilendirilen ve kişisel verileri işleyen üçüncü kişilerin bu bölüm kapsamındaki haklarınıza saygı duymasını sağlamasını talep etme;

8.8. Kişisel verilerin otomatik sistemler vasıtasıyla işlenmesi sonucu ortaya çıkabilecek aleyhte sonuçlara itiraz etme

8.9. Kişisel verilerinizin kanuna aykırı bir şekilde işlenmesi sebebiyle zarara uğramanız halinde bu zararın tazmin edilmesini isteme.

9. **Veri sorumlusuna Başvuru-** Kanunun ilgili kişinin haklarını düzenleyen 11. maddesi kapsamındaki taleplerinizi, "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğe" göre Şirketimizin fiziki adresine adresine yazılı olarak veya üyeliğinizin teyit edildiği elektronik posta üzerinden şirketimiz elektronik posta adresine iletebilirsiniz.

10. **Veri Sorumlusu Bilgilendirmesi -** Aşağıda detaylı kurumsal bilgileri yayınlanan ŞİRKET olarak, 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca Veri Sorumlusu sıfatıyla kişisel verilerinizi ilgili mevzuata uygun olarak kullanacağız.

Veri sorumlusu Unvan	**: EagleBurgmann End. Sız. San. ve Tic. Ltd. Şti.**
Mersis no	**: 0323035768000018**
E-posta adresi	**: kvkk@eagleburgmann.com**
Fiziki Posta adresi	**: Aydınlı-KOSB Mah. Tuzla Kimya San. OSB Tuna Cad. No:8 TR-34953 Tuzla / İstanbul**

KİŞİSEL VERİLERİN KORUNMASI ÇEREZ POLİTİKASI

1. Bu internet sitesine giren kişiler kişisel verilerinin ve özel nitelikteki kişisel verilerinin aşağıda açıklanan amaçlar doğrultusunda kaydedilmesi, işlenmesi, aktarılması, silinmesi, yok edilmesi ve anonimleştirilmesi hakkında bilgilendirilmiş ve kabul etmişlerdir.

2. İşbu bilgilendirme 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun 10.maddesinde düzenlenen Veri sorumlusunun aydınlatma yükümlülüğü hükümleri kapsamında yapılmaktadır.

3. Kişisel Verilerinizin Kaydedilmesi - Aşağıda başlıkları belirtilen kişisel verilerinizi kişisel veri envanterine kişisel veriler politikamızda belirtilen şekillerde kaydedilmektedir.

3.1. IP numarası,
3.2. Konum bilgisi,
3.3. Tarih ve saat bilgisi,
3.4. Cihaz bilgisi,
3.5. Tarayıcı bilgisi,
3.6. Dil bilgisi
3.7. Ülke bilgisi
3.8. Şehir bilgisi
3.9. Geldiği kaynak yer bilgisi,
3.10. İşletim sistemi bilgisi
3.11. Servis sağlayıcı bilgisi,
3.12. Ekran çözünürlüğü bilgisi,
3.13. Ziyaret edilen sayfalar
3.14. Ziyaret edilen sayfalarda geçirilen süre bilgisi,
3.15. Edinme bilgisi,
3.16. Davranış bilgisi
3.17. Dönüşüm bilgisi
3.18. Yönlendiren tarafından bildirilen yaş bilgisi
3.19. Yönlendiren tarafından bildirilen cinsiyet bilgisi
3.20. Site içi arama bilgisi

4. **Kişisel verileriniz nasıl elde edilip kaydedilmektedir?** İnternet sitesinde ziyaretçi bilgileriniz google analytics, sosyal medya ve dijital pazarlama kanalları ve benzeri yazılımlar aracılığıyla elde edilip kaydedilmektedir.

5. **Kişisel verilerinizin işlenmesi;** Bu kapsamda, kişisel verileriniz aşağıdaki amaçlar doğrultusunda özel yazılımlar aracılığıyla işlenmektedir.

5.1. Kurum içerisinde olanların can ve mal güvenliğini korumak
5.2. Türk Ceza Kanunu, Kabahatler Kanunu, Borçlar Kanunu, Türk Ticaret Kanunu, İş Kanunu, 5651 Sayılı Kanun, 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun başta olmak üzere ilgili mevzuat ihlalleri halinde yasayla yetkilendirilmiş kurumlarla, mahkemelerle ve savcılıklarla delil paylaşmak,
5.3. Şirket iç politika veya standart ihlallerinin tespiti, araştırılması ve önlenmesi,
5.4. Şirket'in ana faaliyet konusundaki hizmetleri yönetilmesi ve yürütülmesi,
5.5. Şirket'in sözleşmesel yükümlülüklerinin yerine getirilmesi,
5.6. Verilerin merkezileştirilmesi
5.7. Verilerin analiz edilerek şirket ve internet sitesindeki hizmetlerin geliştirilmesi

6. **Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi.** Kişisel veri envanterimizde yer alan bu veriler, Kişisel Verilerin Korunması Politikamızda düzenlendiği şekilde şirket internet sitesi ziyaret kaydınızın gerçekleştiği tarihin yer aldığı takvim yılının son gününden itibaren **5 yıl sonra** mesai saati bitimine kadar silinecektir.

7. **Kişisel verilerinizin aktarılması,** Şirket ziyaret kaydınızla ilişkin kişisel veriler aşağıdaki kişi ve kuruluşlara aktarılabilecektir.

7.1. Gerçek Kişiler Ve Özel Hukuk Tüzel Kişileri

7.2. Hissedarlar

7.3. İş Ortağı

7.4. İştirak Ve Bağlı Ortaklıklar

7.5. Tedarikçi

7.6. Topluluk Şirketi

7.7. Yetkili Kamu Kurum Ve Kuruluşları

8. **Kişisel Verilerinizin Güvenliği ;** Bilgi Güvenliği Politikasında ve prosedürlerinde Belirtildiği Üzere Şirket Kişisel veri işleme faaliyetlerini yürütürken uygun güvenlik düzeyini temin etmeye yönelik aşağıdaki konulardaki her türlü teknik ve idari tedbirleri almaktadır.

8.1. Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek.

8.2. Kişisel verilere hukuka aykırı olarak erişilmesini önlemek.

8.3. Kişisel verilerin muhafazasını sağlamak.

9. **Haklarınız -** Şirket tarafından verilerinizin işlendiği ve Şirket'in verilerinizi veri sorumlusu sıfatı ile işlediği ölçüde kişisel verileriniz bakımından aşağıda bulunan haklara sahipsiniz:

9.1. Herhangi bir kişisel verinizin işlenip işlenmediğini öğrenme;

9.2. Kişisel verilerinizin işlenme faaliyetlerine ilişkin olarak bilgi talep etme;

9.3. Kişisel verilerinizin işlenme amaçlarını öğrenme;

9.4. Kişisel verilerin yurt içinde veya yurt dışında üçüncü kişilere aktarılmış olması durumunda bu kişileri öğrenme;

9.5. Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme;

9.6. Kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması veya Şirket'in söz konusu verileri işleyebilmek için hukuki dayanağı veya meşru menfaatinin bulunmaması halinde kişisel verilerin silinmesini veya yok edilmesini isteme;

9.7. Şirket'ten, yine Şirket tarafından yetkilendirilen ve kişisel verileri işleyen üçüncü kişilerin bu bölüm kapsamındaki haklarınıza saygı duymasını sağlamasını talep etme;

9.8. Kişisel verilerin otomatik sistemler vasıtasıyla işlenmesi sonucu ortaya çıkabilecek aleyhte sonuçlara itiraz etme

9.9. Kişisel verilerinizin kanuna aykırı bir şekilde işlenmesi sebebiyle zarara uğramanız halinde bu zararın tazmin edilmesini isteme.

10. **Veri Sorumlusu Bilgilendirmesi** - Aşağıda detaylı kurumsal bilgileri yayınlanan **Eagle Burgmann End. Sız. San. ve Tic. Ltd. Sti.** olarak, 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca Veri Sorumlusu sıfatıyla kişisel verilerinizi ilgili mevzuata uygun olarak kullanacağız.

11. **Veri Sorumlusuna Başvuru Usulü** - 6698 sayılı Kişisel Verilerin Korunması Kanunu 13'üncü maddesinin birinci fıkrası uyarınca; veri sorumlusu olan Şirketimize bu haklara ilişkin olarak yapılacak başvuruların yazılı olarak veya Kişisel Verilerin Korunması Kurulu tarafından belirlenen diğer yöntemlerle tarafımıza iletilmesi gerekmektedir. Bu çerçevede "yazılı" olarak Şirketimize yapılacak başvurular aşağıdaki şekilde yapılabilir.

11.1. Başvuru Sahibi'nin şahsen başvurusu ile,

11.2. Noter vasıtasıyla,

11.3. Başvuru Sahibi'nce 5070 Sayılı Elektronik İmza Kanununda tanımlı olan "güvenli elektronik imza" ile imzalanarak Şirket kayıtlı elektronik posta adresine gönderilmek suretiyle,

11.4. İnternet sitesindeki KVK başvuru formu

11.5. Aşağıdaki e-posta adresine gönderilecek e-posta

11.6. Aşağıdaki fiziki posta adresine gönderilecek imzalı posta veya kargo.

Unvan : **Eagle Burgmann End. Sız. San. ve Tic. Ltd. Sti.**
Mersis no :
E-posta adresi : kvkk@eagleburgmann.com
Fiziki Posta adresi : Aydınlı-KOSB Mah. Tuzla Kimya San. OSB
Tuna Cad. No:8 TR-34953 Tuzla / İstanbul
Tel :+90 216 593 02 93-177 Fax :+90 216 593 02 98

EagleBurgmann
a member of EKK and FREUDENBERG

RELY ON EXCELLENCE

BİLGİ GÜVENLİĞİ POLİTİKASI

1. **Amaç :** Bu politikanın amacı, hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek için, üst yönetimin yaklaşımını ve hedeflerini tanımlamak, tüm çalışanlara ve ilgili taraflara bu hedefleri bildirmektir.

2. **Kapsam :** Bu politika Şirket bünyesinde yapılan ticari faaliyetlere ve bu işlemlere ilişkin lojistik, depolama, muhasebe, finans, kalite güvence, satın alma, insan kaynakları, hukuk, satış, pazarlama, iç denetim ve bilgi işlem faaliyetlerinden elde edilen elektronik bilgi varlıkların korunması, şirket bünyesinde tutulan kişisel verilerin kanun kapsamında işlenmesi, saklanması, korunması, gizliliğinin ve bütünlüğünün bozulmaması için kullandığı bilgi güvenliği süreçlerini kapsar.

2.1. **İç Kapsam**

İdare, kuruluşa ilişkin yapı, roller ve yükümlülükler;

2.1.1. Şirket Üst Yönetimi bünyesinde bulunan kapsam dahilindeki departmanlar;, Mali ve İdari İşler, Satınalma, Finans, Bilgi İşlem, Kurumsal İletişim ve İş Geliştirme, İnsan Kaynakları, Kalite, İhracat, İthalat, Lojistik, Hukuk, İç Denetim, Satış, Pazarlama

2.1.2. Genel Yönetim Organizasyon Şemasında belirtilmiş roller ve görev tanımlarındaki sorumluluklar.

2.1.3. Yerine getirilecek politikalar, prosedürler, hedefler ve stratejiler;

2.1.4 Bilgi Güvenliği Yönetim Sistemi Politikası,

2.1.5 Tüm Bilgi Güvenliği yönetim sistemleri prosedürleri,

2.1.6 Yönetimce belirlenmiş yıllık Bilgi Güvenliği yönetim sistemleri hedefleri,

2.1.7 Kaynaklar ve bilgi birikimi cinsinden anlaşılan yetenekler (örneğin, anapara, zaman, kişiler, süreçler, sistemler ve teknolojiler),

2.1.8 Bilgi Güvenliği Yönetim Sisteminin kurulması, işletilmesi ve sürdürülmesi için yönetim tarafından atanan Yönetim Temsilcileri ve Bilgi Güvenliği Yönetim Sistemi ekibi,

2.1.9 İç paydaşlarla ilişkiler ve onların algılamaları ve değerleri, kuruluşun kültürü, kuruluş tarafından uyarlanan standartlar, kılavuzlar ve modeller, sözleşmeye ilişkin ilişkilerin; biçim ve genişliğini kapsamaktadır.

2.2. **Dış Kapsam**

2.2.1 Uluslararası, ulusal, bölgesel veya yerel olmak üzere, sosyal ve kültürel, politik, yasal, mevzuata ilişkin, finansal, teknolojik, ekonomik, doğal ve rekabetçi ortam,

2.2.2 Küresel Rekabet Hukuku, Politikaları ve Prosedürleri,

2.2.3 Tedarikçi ve müşteri verilerinin gizliliği,

2.2.4 Kalite Odaklılık,

2.2.5 Kuruluşun hedefleri üzerinde etkisi bulunan paydaşlarla ilişkiler ve onların algılamaları ve değerleri;

2.2.6 Müşteri memnuniyetin sağlanması için Üst Yönetim dahil tüm Şirket çalışanları,

2.2.7. İlgili tüm yasal mevzuat, düzenleyici, sözleşmeden doğan şartlar, standartlar,

2.2.8 TSE ve diğer kuruluşlarla olan ürün belgelendirmeleri dış kapsamdır

3. **Tanımlar**

3.1. **BGYS:** Bilgi Güvenliği Yönetim Sistemi.

3.2. **Envanter:** Firma için önemli olan her türlü bilgi varlığı.

3.3. **Üst Yönetim:** Şirket Üst Yönetimidir.

3.4. **Know-How:** Bir şeyi yapabilme yetkinliğidir.

3.5. **Bilgi Güvenliği:** Bilgi, tüm diğer kurumsal ve ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun şekilde korunması gereken bir varlıktır. Şirket içerisinde, know-how, süreç, formül, teknik ve yöntem, müşteri kayıtları, pazarlama ve satış bilgileri, personel bilgileri, ticari, sınai ve teknolojik bilgiler ve sırlar GİZLİ BİLGİ olarak kabul edilir.

3.6. **Gizlilik:** Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Örnek: Şifreli e-posta gönderimi ile e-postanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir - Kayıtlı elektronik posta - KEP)

3.7. **Bütünlük:** Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. (Örnek: Veri tabanında saklanan verilerin özet bilgileri ile birlikte saklanması - elektronik imza - mobil imza)

3.8. **Erişilebilirlik/Kullanılabilirlik:** Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Diğer bir ifadeyle, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır. (Örnek: Sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı ve şaselerinde yedekli güç kaynağı kullanımı - UPS). Bu politikada “Erişilebilirlik” olarak kullanılacaktır.

3.9. **Bilgi Varlığı:** Şirket'in sahip olduğu, faaliyetlerini aksatmadan yürütebilmesi için önemli olan varlıklardır. Bu politikaya konu olan süreçler kapsamında bilgi varlıkları şunlardır:

3.9.1. Kağıt, elektronik, görsel veya işitsel ortamda sunulan her türlü bilgi ve veri,

3.9.2. Bilgiye erişmek ve bilgiyi değiştirmek için kullanılan her türlü yazılım ve donanım,

3.9.3. Bilginin transfer edilmesini sağlayan ağlar,

3.9.4. Tesisler ve özel alanlar,

3.9.5. Bölümler, birimler, ekipler ve çalışanlar,

3.9.6. Çözüm ortakları,

3.9.7. Üçüncü taraflardan sağlanan servis, hizmet veya ürünlerdir.

4. **Sorumluluklar** Sorumluluk ve yetkileri belirlenmiş görevlerin nitelik ve yeterlilikleri görev tanımlarında tanımlanmıştır. Bilgi güvenliği ile ilgili faaliyetlerin sürdürülmesinden ve geliştirilmesinden Bilgi İşlem Ekibi ve Yönetim Temsilcisi sorumludur. BGYS Ekibi ve Yönetim Temsilcileri Üst Yönetim tarafından atanmıştır. Kapsam içindeki departmanlardan BGYS temsilcileri belirlenmiştir. BGYS ekip üyesi olarak isim bazında atamaları yapılmıştır

4.1. Yönetim Sorumluluğu

Şirket Yönetimi, tanımlanmış, yürürlüğe konmuş ve uygulanmakta olan Bilgi Güvenliği Sistemine uyacağını ve sistemin verimli şekilde çalışması için gerekli kaynakları tahsis edeceğini, sistemin tüm çalışanlar tarafından anlaşılmasının sağlayacağını taahhüt eder.

4.1.1. BGYS kurulumu sırasında BGYS Yönetim Temsilcisi atama yazısı ile atanır. Gerekli olduğu durumlarda üst yönetim tarafından doküman revize edilerek atama tekrar yapılır.

4.1.2. Yönetim kademesindeki yöneticiler güvenlik konusunda alt kademelerde bulunan personele sorumluluk verme ve örnek olma açısından yardımcı olurlar. Üst kademelerden başlayan ve uygulanan anlayış, firmanın en alt kademe personeline kadar inilmesi zorunludur. Bu yüzden tüm yöneticiler yazılı yada sözlü olarak güvenlik talimatlarına uymaları, güvenlik konularındaki çalışmalara katılmaları yönünde çalışanlarına destek olurlar.

4.1.3. Üst Yönetim, Bilgi güvenliği kapsamlı çalışmalar için gerek duyulan bütçeyi oluşturur.

4.2 Yönetim Temsilcisi Sorumluluğu

4.2.1. BGYS (Bilgi Güvenliği Yönetim Sistemi)'nin planlanması, kabul edilebilir risk seviyesinin belirlenmesi, risk değerlendirme metodolojisinin belirlenmesini,

4.2.2. BGYS kurulumunda destekleyici ve tamamlayıcı faaliyetler için gerekli kaynakların sağlanması, kullanıcı kabiliyetlerinin sağlanması/iyileştirilmesi ve farkındalığın oluşması, eğitimlerin yapılması, iletişimin sağlanması, dokümantasyon gereksinimlerinin sağlanması,

4.2.3. BGYS uygulamalarının yürütülmesi ve yönetilmesi, değerlendirmelerin, iyileştirmelerin ve risk değerlendirmelerinin sürekliliğinin sağlanması,

4.2.4. BGYS uygulamalarının yürütülmesi ve yönetilmesi, değerlendirmelerin, iyileştirmelerin ve risk değerlendirmelerinin sürekliliğinin sağlanması,

4.2.5. İç denetimler, hedeflerin ve yönetim gözden geçirme toplantıları ile BGYS ve kontrollerin değerlendirilmesi,

BGYS'de mevcut yapının sürdürülmesi ve sürekli iyileştirmelerin sağlanmasından sorumludur.

4.3 **BGYS Ekip Üyeleri Sorumluluğu**

4.3.1. Bölümleri ile ilgili varlık envanteri ve risk analiz çalışmalarının yapılması,

4.3.2. Sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik olduğunda, risk değerlendirmesi yapılması için Yönetim Temsilcisini bilgilendirmesi,

4.3.3. Departman çalışanlarının politika ve prosedürlere uygun çalışmasını sağlanması,

4.3.4. İç Denetçi Sorumluluğu İç denetim planı doğrultusunda, görev verilen iç denetimlerde denetim faaliyetlerinin yapılmasından ve raporlanmasından sorumludur.

4.3.5. Bölüm Yöneticileri Sorumluluğu Bilgi Güvenliği Politikasının uygulanması ve çalışanların esaslara uymasının sağlanmasından, 3. tarafların politikadan haberdar olmasının sağlanmasından ve fark ettiği bilgi sistemleri ile ilgili güvenlik ihlal olaylarının bildirilmesinden sorumludurlar.

5. Tüm Çalışanların Sorumluluğu

4.1. Çalışmalarını bilgi güvenliği hedeflerine, politikalarına ve bilgi güvenliği yönetim sistemi dokümanlarına uygun olarak yürütmekten,

4.2. Kendi birimi ile ilgili bilgi güvenliği hedeflerinin takibini yapar ve hedeflere ulaşılmasını sağlar.

4.3. Sistemler veya hizmetlerde gözlenen veya şüphelenilen herhangi bir bilgi güvenliği açıklığına dikkat etmek ve raporlamaktan,

4.4. Üçüncü taraflar ile yapılan ve Satınalma sorumluluğunda olmayan hizmet sözleşmelerine (danışmanlık vb.) ilave olarak gizlilik sözleşmesi yapmak ve bilgi güvenliği gereksinimlerini sağlamaktan sorumludur.

4.5. Üçüncü Tarafların Sorumluluğu Bilgi güvenliği politikasının bilinmesi ve uygulanması ile BGYS kapsamında belirlenen davranışlara uyulmasından sorumludur.

4.6. Bilgi Güvenliği Hedefleri Bilgi Güvenliği Politikası, Şirket çalışanlarına firmanın güvenlik gereksinimlerine uygun şekilde hareket etmesi konusunda yol göstermek, bilinç ve farkındalık seviyelerini arttırmak ve bu şekilde şirketin temel ve destekleyici iş faaliyetlerinin en az kesinti ile devam etmesini sağlamak, güvenilirliğini ve imajını korumak ve üçüncü taraflarla yapılan sözleşmelerde belirlenmiş uygunlukları sağlamak amacıyla firmanın tüm işleyişini etkileyen fiziksel ve elektronik bilgi varlıklarının korunmasını hedefler. Yönetim Tarafından belirlenen hedefler belirlenmiş periyotlarda izlenir ve Yönetim Gözden Geçirme toplantılarında gözden geçirilir.

. **4.7. Risk Yönetim Çerçevesi** Firmanın risk yönetim çerçevesi; Bilgi güvenliği risklerinin tanımlanmasını, değerlendirilmesini ve işlenmesini kapsar. Risk Analizi, uygulanabilirlik bildirgesi ve risk işleme planı, bilgi güvenliği risklerinin nasıl kontrol edildiğini tanımlar. Risk işleme planının yönetiminden ve gerçekleştirilmesinden BGYS Yürütme ve Yönetim Komitesi sorumludur. Tüm bu çalışmalar, varlık envanteri ve risk değerlendirme talimatında detaylı olarak açıklanır.

6. Bilgi Güvenliği Genel Esasları

6.1. Bu politika ile çerçevesi çizilen bilgi güvenliği gereksinimleri ve kurallarına ilişkin ayrıntılar, Şirket çalışanları ve 3. taraflar bu politika ve prosedürleri bilmek ve çalışmalarını bu kurallara uygun şekilde yürütmekle yükümlüdür.

6.2. Bu kural ve politikalar, aksi belirtilmedikçe, basılı veya elektronik ortamda depolanan ve işlenen tüm bilgiler ile bütün bilgi sistemlerinin kullanımı için dikkate alınması esastır.

6.3. Bilgi Güvenliği Yönetim Sistemi, TS ISO/IEC 27001 "Bilgi Teknolojisi Güvenlik Teknikleri (Information Technology Security Techniques) ve Bilgi Güvenliği Yönetim Sistemleri Gereksinimler (Information Security Management Systems Requirements)" standardını temel alarak yapılandırılır ve işletilir.

6.4. BGYS'nin hayata geçirilmesi, işletilmesi ve iyileştirilmesi çalışmalarını, ilgili tarafların katkısıyla yürütür. BGYS dokümanlarının gerektiği zamanlarda güncellenmesi BGYS Yönetim Temsilcisi sorumluluğundadır.

6.5. Şirket tarafından çalışanlara veya 3. taraflara sunulan bilgi sistemleri ve altyapısı ile bu sistemler kullanılarak üretilen her türlü bilgi, belge ve ürün aksini gerektiren kanun hükümleri veya sözleşmeler bulunmadıkça şirkete aittir.

6.6. Çalışanlar, danışmanlık, hizmet alımı (Güvenlik, servis, yemek, temizlik firması vb.), Tedarikçi ve Stajyer ile gizlilik anlaşmaları yapılır.

6.7. İşe alım, görev değişikliği ve işten ayrılma süreçlerinde uygulanacak bilgi güvenliği kontrolleri belirlenir ve uygulanır.

6.8. Çalışanların bilgi güvenliği farkındalığını artıracak ve sistemin işleyişine katkıda bulunmasını sağlayacak eğitimler düzenli olarak mevcut şirket çalışanlarına ve yeni işe başlayan çalışanlara verilir.

6.9. Bilgi güvenliğinin gerçek ya da şüpheli tüm ihlalleri rapor edilir; ihlallere sebep olan uygunsuzluklar tespit edilir, ana sebepleri bulunarak tekrar edilmesini engelleyici önlemler alınır.

6.7. Bilgi varlıklarının envanteri bilgi güvenliği yönetim ihtiyaçları doğrultusunda oluşturulur ve varlık sahiplikleri atanır.

6.8. Kurumsal veriler sınıflandırılır ve her sınıftaki verilerin güvenlik ihtiyaçları ve kullanım kuralları belirlenir.

6.9. Güvenli alanlarda saklanan varlıkların ihtiyaçlarına paralel fiziksel güvenlik kontrolleri uygulanır.

6.10. Firmaya ait bilgi varlıkları için firma içinde ve dışında maruz kalabilecekleri fiziksel tehditlere karşı gerekli kontrol ve politikalar geliştirilir ve uygulanır.

6.11. Kapasite yönetimi, üçüncü taraflarla ilişkiler, yedekleme, sistem kabulü ve diğer güvenlik süreçlerine ilişkin prosedür ve talimatlar geliştirilir ve uygulanır.

6.12. Ağ cihazları, işletim sistemleri, sunucular ve uygulamalar için denetim kaydı üretme konfigürasyonları ilgili sistemlerin güvenlik ihtiyaçlarına paralel biçimde ayarlanır. Denetim kayıtlarının yetkisiz erişime karşı korunması sağlanır.

6.13. Erişim hakları ihtiyaç nispetinde atanır. Erişim kontrolü için mümkün olan en güvenli teknoloji ve teknikler kullanılır.
6.14. Sistem temini ve geliştirilmesinde güvenlik gereksinimleri belirlenir, sistem kabulü veya testlerinde güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilir.
6.15. Kritik altyapı için süreklilik planları hazırlanır, bakımı ve tatbikatı yapılır.
6.16. Yasalara, iç politika ve prosedürlere, teknik güvenlik standartlarına uyum için gerekli süreçler tasarlanır, sürekli ve periyodik olarak yapılacak gözetim ve denetim faaliyetleri ile uyum güvencesi sağlanır.
7. Politikanın İhlali ve Yaptırımlar Bilgi Güvenliği Politikasına ve Standartlarına uyulmadığının tespit edilmesi durumunda, bu ihlalden sorumlu olan çalışanlar için Disiplin Yönergesi ve Prosedürü 'ne göre 3. Taraflar için de geçerli olan sözleşmelerde geçen ilgili maddelerinde belirlenen yaptırımlar uygulanır.
8. Yönetimin Gözden Geçirmesi Yönetim gözden geçirme toplantıları BGYS Kalite Yönetim Temsilcisi Organize edilerek, Üst Yönetim ve Bölüm yöneticileri katılımı ile gerçekleştirilir. Bilgi Güvenliği Yönetim Sisteminin uygunluğunun ve etkinliğinin değerlendirildiği bu toplantılar en az yılda bir kez gerçekleştirilmektedir.
9. Bilgi Güvenliği Politika Dokümanı Güncellenmesi ve Gözden Geçirilmesi Politika dokümanının sürekliliğinin sağlanmasından ve gözden geçirilmesinden BGYS Yönetim Temsilcileri sorumludur. Politika ve prosedürler en az yılda bir kez gözden geçirilmelidir. Bunun dışında sistem yapısını veya risk değerlendirmesini etkileyecek herhangi bir değişiklikten sonra da gözden geçirilmeli ve herhangi bir değişiklik gerekiyorsa üst yönetime onaylatılarak yeni versiyon olarak kayıt altına alınmalıdır. Her revizyon tüm kullanıcıların erişebileceği şekilde yayınlanmalıdır.

KİŞİSEL VERİLERİN KORUNMASI POLİTİKASI

1. **Yasal Dayanak :** Anayasa'nın 20. maddesinde düzenlenen; herkesin, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu, bu hakkın; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsadığını, kişisel verilerin, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceğini temel yasal dayanak alarak 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca Kişisel Verilerin hukuka uygun olarak korunması ve işlenmesine azami önem veriyor ve tüm planlama ve faaliyetlerimizde bu özenle hareket ediyoruz. Şirket olarak, özel hayatın gizliliğinin temeli olan Kişisel Verilerin korunması ve ve işlenmesi için tüm idari ve teknik tedbirleri alıyor personelimize 5237 sayılı Türk Ceza Kanununun (TCK) 135.madde ve devamında düzenlenen yasal yaptırımlar konusunda bilgilendirme ve uyarılarda bulunuyoruz.

2. **Amaç:** Yürürlükte bulunan 6698 sayılı Kişisel Verilerin Korunması hakkındaki Kanunu ile, kişisel verilerin işlenmesinde, başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerinin korunması ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esaslar düzenlenmiştir. Söz konusu düzenleme de dikkate alınarak hazırlanan politikamızın amacı; kişisel verilerin korunması hakkındaki yükümlülüklere uyumun sağlanması, Şirketimizin gerçekleştirdiği faaliyetler kapsamında temin edilen bilgilerin işlenmesi, aktarılması ve gizliliğinin korunması ile ilgili hususların risk temelli bir yaklaşımla değerlendirilerek, stratejilerin, kurum içi kontrol ve önlemlerin, işleyiş kurallarının ve sorumlulukların belirlenmesi ile kurum çalışanlarının bu konularda bilinçlendirilmesidir. Aynı zamanda; müşterilerimiz, potansiyel müşterilerimiz, çalışanlarımız, çalışan adaylarımız, Şirket hissedarlarımız, Şirket yetkililerimiz, ziyaretçilerimiz, işbirliği içinde olduğumuz kurum/kuruluşların çalışanları, hissedarları ve yetkilileri ve üçüncü kişiler başta olmak üzere kişisel verileri Şirketimiz tarafından işlenen kişileri bilgilendirilerek şeffaflığı sağlamak amaçlanmaktadır.

3. **Kapsam:** Bu politika; müşterilerimizin, potansiyel müşterilerimizin, çalışanlarımızın, çalışan adaylarımızın, Şirket hissedarlarının, Şirket yetkililerinin, ziyaretçilerimizin, işbirliği içinde olduğumuz kurumların çalışanları, hissedarları ve yetkililerinin ve üçüncü kişilerin otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen tüm kişisel verilerine ilişkindir.

4. **Tanımlar**

4.1. **Açık Rıza** Belirli bir konuya ilişkin bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.

4.2. **Anonim Hale Getirme** Kişisel verinin, kimliği belli veya belirlenebilir biri ile ilişkilendirilebilme niteliğini kaybedecek ve bu durumun geri alınamayacağı şekilde değiştirilmesidir. Örnek: Maskeleme, toplulaştırma, veri bozma vb. tekniklerle kişisel verinin bir gerçek kişi ile ilişkilendirilemeyecek hale getirilmesi.

4.3. **Çalışan** Şirket ile arasında yapılmış olan iş akdi gereğince Şirkette çalışmakta olan kişiler

4.4. **Çalışan Adayı** Şirket ya herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini Şirketin incelemesine açmış olan gerçek kişiler

4.5. **İşbirliği İçerisinde Olduğumuz Kurumların Çalışanları, Hissedarları ve Yetkilileri** Şirketin her türlü iş ilişkisi içerisinde bulunduğu kurumlarda (iş ortağı, tedarikçi gibi, ancak bunlarla sınırlı olmaksızın) çalışan, bu kurumların hissedarları ve yetkilileri dahil olmak üzere, gerçek kişiler

4.6. **Kişisel Verilerin İşlenmesi:** 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 veriler üzerinde gerçekleştirilen her türlü işlem.

4.7. **Kişisel Veri Sahibi** Kişisel verisi işlenen gerçek kişi. Örneğin; Müşteriler ve çalışanlar.

4.8. **Kişisel Veri** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi. Tüzel kişilere ilişkin bilgilerin işlenmesi kanun kapsamında değildir. Örneğin; ad-soyadı, TC, e-posta, adres, doğum tarihi, kredi kartı numarası vb.

4.9. **Müşteri** Şirket ile herhangi bir sözleşmesel ilişkisi olup olmadığına bakılmaksızın Şirketin sunmuş olduğu ürün ve hizmetleri kullanan veya kullanmış olan gerçek kişiler

4.10. **Özel Nitelikli Kişisel Veri :** Irk, etnik köken, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançlar, kılık kıyafet, dernek vakıf ya da sendika üyeliği, sağlık, cinsel hayat, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili veriler ile biyometrik ve genetik veriler özel nitelikli verilerdir.

4.11. **Potansiyel Müşteri** Ürün ve hizmetlerimize kullanma talebinde veya ilgisinde bulunmuş veya bu ilgiye sahip olabileceği ticari teamül ve dürüstlük kurallarına uygun olarak değerlendirilmiş gerçek kişiler

4.12. **Şirket Hissedarı:** Şirketin hissedarı gerçek kişiler

4.13. **Şirket Yetkilisi:** Şirketin yönetim kurulu üyesi ve diğer yetkili gerçek kişiler

Üçüncü Kişi Şirketin yukarıda bahsi geçen taraflarla arasındaki ticari işlem güvenliğini sağlamak veya bahsi geçen kişilerin haklarını korumak ve menfaat temin etmek üzere bu kişilerle ilişkili olan üçüncü taraf gerçek kişiler (Örn. Aile Bireyleri ve yakınlar)

4.14. **Veri İşleyen** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek ve tüzel kişidir. Örneğin, Şirketin verilerini tutan firma veya şirketler vb.

4.15. **Veri Sorumlusu** Kişisel verilerin işlenme amaçlarını ve vasıtalarını belirleyen, verilerin sistematik bir şekilde tutulduğu yeri (veri kayıt sistemi) yöneten, veri sahibinin talebi / başvurusu neticesinde kişisel bilgileri ile ilgili veri sahibine gerekli bilgiyi sağlayan ve yönlendirmeleri yapan kişi veri sorumlusudur.

4.16. **Ziyaretçi** Şirketin sahip olduğu fiziksel yerleşkelere çeşitli amaçlarla girmiş olan veya internet sitelerimizi ziyaret eden gerçek kişiler

5. **Kısaltmalar**

5.1. **KVKK :** 6698 sayılı Kanun 7 Nisan 2016 tarihli ve 29677 sayılı Resmi Gazete 'de yayımlanan, 24 Mart 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu.

5.2. **Anayasa :** 9 Kasım 1982 tarihli ve 17863 sayılı Resmi Gazete 'de yayımlanan; 7 Kasım 1982 tarihli ve 2709 sayılı Türkiye Cumhuriyeti Anayasası.

5.3. KVK Kurulu Kişisel Verileri Koruma Kurulu

5.4. KVK Kurumu Kişisel Verileri Koruma Kurumu

5.5. Politika Şirket Kişisel Verilerin Korunması ve İşlenmesi Politikası

5.6. TBK 4 Şubat 2011 tarihli ve 27836 sayılı Resmi Gazete 'de yayımlanan; 11 Ocak 2011 tarihli ve 6098 sayılı Türk Borçlar Kanunu.

5.7. TCK 12 Ekim 2004 tarihli ve 25611 sayılı Resmi Gazete 'de yayımlanan; 26 Eylül 2004 tarihli ve 5237 sayılı Türk Ceza Kanunu.

5.8. TTK 14 Şubat 2011 tarihli ve 27846 sayılı Resmi Gazete 'de yayımlanan;13 Ocak 2011 tarihli ve 6102 sayılı Türk Ticaret Kanunu

6. **Veri Kategorileri:** Şirket aşağıdaki veri kategorilerine ilişkin verileri kaydedebilir, işleyebilir veya aktarabilir.

6.1. Kimlik (ad soyad, anne - baba adı, doğum tarihi, doğum yeri, medeni hali,nüfus cüzdanı seri sıra no, tc kimlik no)

6.2. İletişim (adres no, e-posta adresi, iletişim adresi, kayıtlı elektronik posta adresi (KEP), telefon no)

6.3. Özlük (bordro bilgileri, disiplin soruşturması, işe giriş-çıkış belgesi kayıtları, özgeçmiş bilgileri, performans değerlendirme raporları)

6.4. **Hukuki İşlem** (adli makamlarla yazışmalardaki bilgiler, dava dosyasındaki bilgiler)

6.5. **Müşteri İşlem** (fatura, senet, çek bilgileri, sipariş bilgisi, talep bilgisi)

6.6. **Fiziksel Mekân** Güvenliği (çalışan ve ziyaretçilerin giriş çıkış kayıt bilgileri, kamera kayıtları

6.7. **İşlem Güvenliği** (IP adresi bilgileri, internet sitesi giriş çıkış bilgileri, şifre ve parola bilgileri)

6.8. **Risk Yönetimi** (ticari, teknik, idari risklerin yönetilmesi için işlenen bilgiler)

6.9. **Finans** (bilanço bilgileri, finansal performans bilgileri, kredi ve risk bilgileri, mal varlığı bilgileri)

6.10. **Mesleki Deneyim** (diploma bilgileri, gidilen kurslar, meslek içi eğitim bilgileri, sertifikalar, transkript bilgileri)

6.11. **Pazarlama** (anket, çerez kayıtları, kampanya çalışmasıyla elde edilen bilgiler)

6.12. **Görsel ve İşitsel Kayıtlar** (görsel ve işitsel kayıtlar)

6.13. **Kılık ve Kıyafet:** (Kılık ve kıyafete ilişkin bilgiler)

6.14. **Sağlık Bilgileri** (engellilik durumuna ait bilgiler, kan grubu bilgisi, kişisel sağlık bilgileri, kullanılan cihaz ve protez bilgileri)

6.15. **Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri** (ceza mahkûmiyetine ilişkin bilgiler, güvenlik tedbirlerine ilişkin bilgiler)

6.16. **Biyometrik Veri** (yüz tanıma bilgileri)

7. **Kişisel Veri İşleme Amaçları** Şirket aşağıdaki amaçlara göre kişisel verileri kaydedebilir, işleyebilir veya aktarabilir.

7.1. Acil Durum Yönetimi Süreçlerinin Yürütülmesi

7.2. Bilgi Güvenliği Süreçlerinin Yürütülmesi

7.3. Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
7.4. Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
7.5. Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi
7.6. Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
7.7. Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
7.8. Denetim / Etik Faaliyetlerinin Yürütülmesi
7.9. Eğitim Faaliyetlerinin Yürütülmesi
7.10. Erişim Yetkilerinin Yürütülmesi
7.11. Faaliyetlerin Mevzuata Uygun Yürütülmesi
7.12. Finans Ve Muhasebe İşlerinin Yürütülmesi
7.13. Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi
7.14. Fiziksel Mekan Güvenliğinin Temini
7.15. Görevlendirme Süreçlerinin Yürütülmesi
7.16. Hukuk İşlerinin Takibi Ve Yürütülmesi
7.17. İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
7.18. İletişim Faaliyetlerinin Yürütülmesi
7.19. İnsan Kaynakları Süreçlerinin Planlanması
7.20. İş Faaliyetlerinin Yürütülmesi / Denetimi
7.21. İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
7.22. İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi
7.23. İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
7.24. Lojistik Faaliyetlerinin Yürütülmesi
7.25. Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
7.26. Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
7.27. Mal / Hizmet Satış Süreçlerinin Yürütülmesi
7.28. Mal / Hizmet Üretim Ve Operasyon Süreçlerinin Yürütülmesi
7.29. Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
7.30. Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi
7.31. Organizasyon Ve Etkinlik Yönetimi
7.32. Pazarlama Analiz Çalışmalarının Yürütülmesi
7.33. Performans Değerlendirme Süreçlerinin Yürütülmesi
7.34. Reklam / Kampanya / Promosyon Süreçlerinin Yürütülmesi
7.35. Risk Yönetimi Süreçlerinin Yürütülmesi
7.36. Saklama Ve Arşiv Faaliyetlerinin Yürütülmesi
7.37. Sosyal Sorumluluk Ve Sivil Toplum Aktivitelerinin Yürütülmesi
7.38. Sözleşme Süreçlerinin Yürütülmesi
7.39. Sponsorluk Faaliyetlerinin Yürütülmesi
7.40. Stratejik Planlama Faaliyetlerinin Yürütülmesi
7.41. Talep / Şikayetlerin Takibi
7.42. Taşınır Mal Ve Kaynakların Güvenliğinin Temini
7.43. Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
7.44. Ücret Politikasının Yürütülmesi
7.45. Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
7.46. Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
7.47. Yabancı Personel Çalışma Ve Oturma İzni İşlemleri
7.48. Yatırım Süreçlerinin Yürütülmesi
7.49. Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi
7.50. Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
7.51. Yönetim Faaliyetlerinin Yürütülmesi
7.52. Ziyaretçi Kayıtlarının Oluşturulması Ve Takibi

8. **Kişisel Veri Aktarım Alıcı Grupları** Şirket aşağıdaki Kişisel Veri Aktarı Alıcı gruplarına kişisel verileri aktarabilir.
   - **8.1.** Gerçek Kişiler Ve Özel Hukuk Tüzel Kişileri
   - **8.2.** Herkese Açık
   - **8.3.** Hissedarlar
   - **8.4.** İş Ortağı
   - **8.5.** İştirak Ve Bağlı Ortaklıklar
   - **8.6.** Tedarikçi
   - **8.7.** Topluluk Şirketi
   - **8.8.** Yetkili Kamu Kurum Ve Kuruluşları
9. **Kişisel Veri Konusu Kişiler -** Şirket aşağıdaki kişi türlerine göre kişisel verileri kaydedebilir, işleyebilir veya aktarabilir.
   - **9.1.** Çalışan Adayı
   - **9.2.** Çalışan
   - **9.3.** Hissedar/Ortak
   - **9.4.** Potansiyel Ürün Ve Hizmet Alıcısı
   - **9.5.** Stajyer
   - **9.6.** Tedarikçi Çalışan
   - **9.7.** Tedarikçi Yetkilisi
   - **9.8.** Ürün Veya Hizmet Alan Kişi
   - **9.9.** Ziyaretçi
10. **Kişisel Veri Saklama Süreleri :** Kişisel verileri saklama süreleri Kişisel veri Saklama ve İmha politikasında ayrıntılı olarak düzenlenmiştir.
11. **Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi :**
    - **11.1.** Kişisel verilerin hukuka uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde bu veriler, resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir.
    - **11.2.** Veri sorumlusu, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.
    - **11.3.** Bu hususlara ilişkin yapılması gereken işlemler Kişisel veri saklama ve imha politikasında ayrıntılı olarak açıklanmıştır.
12. **Kişisel Verilerin Aktarılması** Kanunda belirtilen genel ilkeler çerçevesinde işlenmek üzere elde edilen kişisel veriler, ilgili kişinin açık rızası alınmak suretiyle üçüncü kişilere aktarılabilir.
    - **12.1. Yurt içi aktarım:** Kişisel veri ve özel nitelikteki kişisel verilerin yurt içinde aktarımına ilişkin ayrıntılar Kişisel Verilerin Aktarılması prosedüründe düzenlenmiştir.
    - **12.2 Yurt dışı aktarım :** İlgili kişinin açık rızasının bulunması şartıyla Kanunda belirtilen hallerin varlığı halinde Yeterli korumanın bulunduğu ülkelere kişisel veri aktarımı yapılabilir. Yeterli korumanın bulunmadığı ülkelere veri aktarımı ise Kanunda belirtilen hallerin varlığı, açık rızanın olmasına ek olarak yeterli korumanın yazılı olarak taahhüt edilmesi ve Kurulun izninin bulunması durumlarında gerçekleştirilebilir. Konuya ilişkin ayrıntılar Kişisel Verilerin Aktarılması Prosedürü'nde düzenlenmiştir.
13. **Kişisel Verilerin İşlenmesinde Genel (Temel) İlkeler:** Kişisel veriler Kişisel verilerin işlenmesi prosedüründe ayrıntılı olarak belirtildiği şekilde aşağıdaki temel ilkelere uygun olarak işlenecektir.
    - **13.1.** Hukuka ve dürüstlük kurallarına uygun olma,
    - **13.2.** Doğru ve gerektiğinde güncel olma,
    - **13.3.** Belirli, açık ve meşru amaçlar için işlenme,
    - **13.4.** İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
    - **13.5.** İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.
14. **Açık Rıza :** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır. Açık rıza alma prosedüründe ayrıntılı olarak belirtildiği üzere Açık rıza'nın Belirli bir konuya ilişkin olması, Rızanın bilgilendirmeye dayanması ve Özgür iradeyle açıklanması gereklidir.
15. **Aydınlatma yükümlülüğü :** Kişisel verilerin elde edilmesi sırasında şirket tarafından ilgili kişilerin bilgilendirilir. Aydınlatma Prosedüründe ayrıntılı olarak düzenlendiği üzere bu bilgilendirme asgari olarak aşağıdaki konuları içermektedir.
    - **15.1.** Veri sorumlusunun ve varsa temsilcisinin kimliği,
    - **15.2.** Kişisel verilerin hangi amaçla işleneceği,
    - **15.3.** Kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
    - **15.4.** Kişisel veri toplamanın yöntemi ve hukuki sebebi,

15.5. İlgili kişinin Kanunun 11 inci maddesinde sayılan diğer hakları.

16. **İlgili kişinin hak arama yöntemleri:** İlgili kişilerin, Şirkete başvurarak; kendileriyle ilgili kişisel verilerin işlenip işlenmediğini öğrenmek, işlenmişse bunları talep etmek, verinin muhtevasının eksik veya yanlış olması halinde bunların düzeltilmesini, hukuka aykırı olması halinde ise silinmesini, yok edilmesini ve buna göre yapılacak işlemlerin verilerin açıklandığı üçüncü kişilere bildirilmesini ve verilerin kanuna aykırı olarak işlenmesi sebebiyle zararlarının giderilmesini talep etme hakları bulunmaktadır. İlgili kişi ayrıntıları İlgili Kişinin Hak Arama Prosedürü'nde belirtildiği üzere başvuru ve şikayet haklarını kullanabilir.

16.1. **Başvuru :** İlgili kişilerin, sahip oldukları hakları kullanabilmeleri için öncelikle veri sorumlusuna başvurmaları zorunludur. Bu yol tüketilmeden Kurula şikâyet yoluna gidilemez.

16.2. **Şikayet :** İlgili kişinin şikayet yoluna başvurulabilmesi için Şirkete başvurunun reddedilmesi, verilen cevabın yetersiz bulunması veya 30 gün içinde başvuruya cevap verilmemiş olması gereklidir. İlgili kişilerin Şirkete başvurmadan doğrudan Kurula şikayet yoluna gitmesi mümkün değildir.

17. **Kurul Kararlarının Yerine Getirilmesi Yükümlülüğü :** Kurul, şikâyet üzerine veya ihlal iddiasını öğrenmesi durumunda resen görev alanına giren konularda yapacağı inceleme sonucunda bir ihlalin varlığını tespit ederse, hukuka aykırılıkların Şirket tarafından giderilmesine karar vererek, kararı ilgililere tebliğ eder. Kurul Kararlarının Yerine Getirilmesi prosedüründe ayrıntılı olarak belirtildiği üzere Şirket, bu kararı, tebliğ tarihinden itibaren gecikmeksizin ve en geç otuz gün içinde yerine getirir.

18. **Veri Sorumluları Sicili (VERBİS) kayıt yükümlülüğü:** Şirket , Veri sorumlularının kayıt olmak zorunda oldukları ve veri işleme faaliyetleri ile ilgili bilgileri beyan ettikleri kayıt sistemine Veri Sorumluları Sicili (VERBİS) kayıt prosedüründe belirtildiği şekilde kayıt olur ve bu kayıtları günceller.

19. **Kişisel Veri İhlali :** İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, Şirket bu durumu en kısa sürede Kişisel Veri İhlali Prosedüründe belirtildiği şekilde ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

20. **Kişisel Veri Güvenliği Tedbirleri :** Şirket Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek, Kişisel verilere hukuka aykırı olarak erişilmesini önlemek, Kişisel verilerin muhafazasını sağlamak için aşağıdaki teknik ve idari tedbirleri Şirket yapısına uygun düzeyde almaktadır.

20.1. Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

20.2. Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.

20.3. Anahtar yönetimi uygulanmaktadır.

20.4. Bilgi teknolojileri sistemleri tedarik, gelistirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.

20.5. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

20.6. Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

20.7. Çalışanlar için yetki matrisi oluşturulmuştur.

20.8. Erişim logları düzenli olarak tutulmaktadır.

20.9. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.

20.10. Gerektiğinde veri maskeleme önlemi uygulanmaktadır.

20.11. Gizlilik taahhütnameleri yapılmaktadır.

20.12. Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

20.13. Güncel anti-virüs sistemleri kullanılmaktadır.

20.14. Güvenlik duvarları kullanılmaktadır.

20.15. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.

20.16. Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.

20.17. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.

20.18. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.

20.19. Kişisel veri güvenliğinin takibi yapılmaktadır.

20.20. Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.

20.21. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.

20.22. Kişisel veri içeren ortamların güvenliği sağlanmaktadır.

20.23. Kişisel veriler mümkün olduğunca azaltılmaktadır.

20.24. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.

20.25. Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
20.26. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
20.27. Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
20.28. Mevcut risk ve tehditler belirlenmiştir.
20.29. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
20.30. Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
20.31. Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.
20.32. Saldırı tespit ve önleme sistemleri kullanılmaktadır.
20.33. Sızma testi uygulanmaktadır.
20.34. Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.
20.35. Şifreleme yapılmaktadır.
20.36. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.
20.37. Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.
20.38. Veri kaybı önleme yazılımları kullanılmaktadır.

EagleBurgmann
a member of EKK and FREUDENBERG

RELY ON EXCELLENCE

KİŞİSEL VERİLERİN KORUNMASI SAKLAMA VE İMHA POLİTİKASI

1. Bu politikanın amacı, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin usul ve esasları belirlemektir.

2. Bu politika; 6698 sayılı Kanunun 7 nci maddesinin üçüncü fıkrası ile 22 nci maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanmış Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Yönetmeliğine uygun olarak hazırlanmıştır.

3. Şirket; Kişisel veri işleme envanterine uygun olarak bu kişisel veri saklama ve imha politikasını hazırlamıştır.

4. Tanımlar

4.1. Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.

4.2. İlgili kullanıcı: Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileridir

4.3. İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi işlemidir.

4.4. Kayıt ortamı: Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı ifade eder.

4.5. Kişisel veri işleme 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 envanterdir.

4.6. Kişisel veri saklama ve imha politikası: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikadır.

4.7. 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 ifade eder.

4.8. Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini ifade eder.

4.9. Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.

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

4.11. Kişisel verilerin silinmesi Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

4.12. Kişisel verilerin yok edilmesi Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

4.13. Kişisel verilerin anonim hale getirilmesi Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.

5. Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamları :

5.1. Kağıt ortamlar

5.1.1. Kağıt

5.1.2. Manuel veri kayıt sistemleri (formlar ziyaretçi giriş defteri)

5.1.3. Yazılı, basılı, görsel ortamlar

5.2. Elektronik ortamlar

5.2.1. Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.)

5.2.2. Yazılımlar
5.2.3. Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.)
5.2.4. Kişisel bilgisayarlar (Masaüstü, dizüstü)
5.2.5. Mobil cihazlar (telefon, tablet vb.)
5.2.6. Optik diskler (CD, DVD vb.)
5.2.7. Çıkartılabilir bellekler (USB, Hafıza Kart vb.)
5.2.8. Yazıcı, tarayıcı, fotokopi makinesi

6. Saklamayı Gerektiren Hukuki Sebepler

6.1. 6698 sayılı Kişisel Verilerin Korunması Kanunu,
6.2. 6098 sayılı Türk Borçlar Kanunu,
6.3. 4734 sayılı Kamu İhale Kanunu,
6.4. 657 sayılı Devlet Memurları Kanunu,
6.5. 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
6.6. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar
6.7. Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
6.8. 5018 sayılı Kamu Mali Yönetimi Kanunu,
6.9. 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
6.10. 4982 Sayılı Bilgi Edinme Kanunu,
6.11. 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun
6.12. 4857 sayılı İş Kanunu,
6.13. 2547 sayılı Yükseköğretim Kanunu,
6.14. 5434 sayılı Emekli Sağlığı Kanunu,
6.15. 2828 sayılı Sosyal Hizmetler Kanunu
6.16. İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
6.17. Arşiv Hizmetleri Hakkında Yönetmelik
6.18. Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

7. Saklamayı Gerektiren İşleme Amaçları

7.1. Acil Durum Yönetimi Süreçlerinin Yürütülmesi
7.2. Bilgi Güvenliği Süreçlerinin Yürütülmesi
7.3. Çalışan Adayı / Stajyer / Öğrenci Seçme Ve Yerleştirme Süreçlerinin Yürütülmesi
7.4. Çalışan Adaylarının Başvuru Süreçlerinin Yürütülmesi
7.5. Çalışan Memnuniyeti Ve Bağlılığı Süreçlerinin Yürütülmesi
7.6. Çalışanlar İçin İş Akdi Ve Mevzuattan Kaynaklı Yükümlülüklerin Yerine Getirilmesi
7.7. Çalışanlar İçin Yan Haklar Ve Menfaatleri Süreçlerinin Yürütülmesi
7.8. Denetim / Etik Faaliyetlerinin Yürütülmesi
7.9. Eğitim Faaliyetlerinin Yürütülmesi
7.10. Erişim Yetkilerinin Yürütülmesi
7.11. Faaliyetlerin Mevzuata Uygun Yürütülmesi
7.12. Finans Ve Muhasebe İşlerinin Yürütülmesi
7.13. Firma / Ürün / Hizmetlere Bağlılık Süreçlerinin Yürütülmesi
7.14. Fiziksel Mekan Güvenliğinin Temini
7.15. Görevlendirme Süreçlerinin Yürütülmesi
7.16. Hukuk İşlerinin Takibi Ve Yürütülmesi
7.17. İç Denetim/ Soruşturma / İstihbarat Faaliyetlerinin Yürütülmesi
7.18. İletişim Faaliyetlerinin Yürütülmesi
7.19. İnsan Kaynakları Süreçlerinin Planlanması
7.20. İş Faaliyetlerinin Yürütülmesi / Denetimi
7.21. İş Sağlığı / Güvenliği Faaliyetlerinin Yürütülmesi
7.22. İş Süreçlerinin İyileştirilmesine Yönelik Önerilerin Alınması Ve Değerlendirilmesi

7.23. İş Sürekliliğinin Sağlanması Faaliyetlerinin Yürütülmesi
7.24. Lojistik Faaliyetlerinin Yürütülmesi
7.25. Mal / Hizmet Satın Alım Süreçlerinin Yürütülmesi
7.26. Mal / Hizmet Satış Sonrası Destek Hizmetlerinin Yürütülmesi
7.27. Mal / Hizmet Satış Süreçlerinin Yürütülmesi
7.28. Mal / Hizmet Üretim Ve Operasyon Süreçlerinin Yürütülmesi
7.29. Müşteri İlişkileri Yönetimi Süreçlerinin Yürütülmesi
7.30. Müşteri Memnuniyetine Yönelik Aktivitelerin Yürütülmesi
7.31. Organizasyon Ve Etkinlik Yönetimi
7.32. Pazarlama Analiz Çalışmalarının Yürütülmesi
7.33. Performans Değerlendirme Süreçlerinin Yürütülmesi
7.34. Reklam / Kampanya / Promosyon Süreçlerinin Yürütülmesi
7.35. Risk Yönetimi Süreçlerinin Yürütülmesi
7.36. Saklama Ve Arşiv Faaliyetlerinin Yürütülmesi
7.37. Sosyal Sorumluluk Ve Sivil Toplum Aktivitelerinin Yürütülmesi
7.38. Sözleşme Süreçlerinin Yürütülmesi
7.39. Sponsorluk Faaliyetlerinin Yürütülmesi
7.40. Stratejik Planlama Faaliyetlerinin Yürütülmesi
7.41. Talep / Şikayetlerin Takibi
7.42. Taşınır Mal Ve Kaynakların Güvenliğinin Temini
7.43. Tedarik Zinciri Yönetimi Süreçlerinin Yürütülmesi
7.44. Ücret Politikasının Yürütülmesi
7.45. Ürün / Hizmetlerin Pazarlama Süreçlerinin Yürütülmesi
7.46. Veri Sorumlusu Operasyonlarının Güvenliğinin Temini
7.47. Yabancı Personel Çalışma Ve Oturma İzni İşlemleri
7.48. Yatırım Süreçlerinin Yürütülmesi
7.49. Yetenek / Kariyer Gelişimi Faaliyetlerinin Yürütülmesi
7.50. Yetkili Kişi, Kurum Ve Kuruluşlara Bilgi Verilmesi
7.51. Yönetim Faaliyetlerinin Yürütülmesi
7.52. Ziyaretçi Kayıtlarının Oluşturulması Ve Takibi

8. İmhayı Gerektiren Sebepler

8.1. Kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir.

8.2. Türk Ceza Kanunu'nun 138. maddesinde ve KVK Kanunu'nun 7. maddesinde düzenlendiği üzere ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde Şirket kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel veriler silinir, yok edilir veya anonim hale getirilir.

8.3. İlgili kişi, Şirkete başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde bu talebi yerine getirilmek üzere hemen değerlendirmeye alınır.

8.4. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Şirket, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.

8.5. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa Şirket bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu politika kapsamında gerekli işlemlerin yapılmasını temin eder.

8.6. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

9. Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirler

9.1. Teknik Tedbirler

9.1.1. Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.

9.1.2. Ağ yoluyla veri akarımlarında kapalı sistem ağ kullanılmaktadır.

9.1.3. Anahtar yönetimi uygulanmaktadır.

9.1.4. Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.

9.1.5. Çalışanlar için yetki matrisi oluşturulmuştur.

9.1.6. Erişim logları düzenli olarak tutulmaktadır.

9.1.7. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.

9.1.8. Gerektiğinde veri maskeleme yöntemi uygulanmaktadır.

9.1.9. Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.

9.1.10. Kişisel veri güvenliğinin takibi yapılmaktadır.

9.1.11. Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.

9.1.12. Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır

9.1.13. Kişisel veri içeren ortamların güvenliği sağlanmaktadır.

9.1.14. Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.

9.1.15. Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.

9.1.16. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

9.1.17. Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.

9.1.18. Mevcut risk ve tehditler belirlenmiştir.

9.1.19. Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.

9.1.20. Özel nitelikli kişisel veriler için güvenli şifreleme / kriptografik anahtarlar kullanılmakta ve farklı birimlerce yönetilmektedir.

9.1.21. Saldırı tespit ve önleme sistemleri kullanılmaktadır.

9.1.22. Sızma testi uygulanmaktadır.

9.1.23. Siber güvenlik önlemleri alınmış olup uygulanması sürekli takip edilmektedir.

9.1.24. Şifreleme yapılmaktadır.

9.1.25. Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklara denetimi sağlanmaktadır.

9.1.26. Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır.

9.1.27. Veri kaybı önleme yazılımları kullanılmaktadır.

9.2. İdari Tedbirler

9.2.1. Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.

9.2.2. Çalışanlar için veri güvenliği konusunda belirli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.

9.2.3. Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulanmaya başlanmıştır.

9.2.4. Gizlilik taahhütnameleri yapılmaktadır.

9.2.5. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.

9.2.6. Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.

9.2.7. Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.

9.2.8. Kişisel veri içeren ortamların güvenliği sağlanmaktadır.

9.2.9. Kişisel veriler mümkün olduğunca azaltılmaktadır.

9.2.10. Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.

9.2.11. Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler mevcuttur.

10. Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirler

10.1. Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili bütün işlemler yetkili kişiler tarafından politika ve prosedürlere uygun olarak yapılır ve kayıt altına alınır.

10.2. Söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

11. Kişisel Verilerin Silinmesi, Yok Edilmesi ve Anonimleştirilmesi Teknikleri

11.1 Fiziksel Olarak Yok Etme Kişisel veriler herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla da işlenebilmektedir. Bu tür veriler silinirken/yok edilirken kişisel verinin sonradan kullanılamayacak biçimde fiziksel olarak yok edilmesi sistemi uygulanmaktadır. Örnek: İlgili dosyanın, belgenin parçalanarak çöpe atılması.

11.2 Yazılımdan Güvenli Olarak Silme Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; çok yüksek ihtimalle bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

11.3 Uzman Tarafından Güvenli Olarak Silme Şirket bazı durumlarda kendisi adına kişisel verileri silmesi için bir uzman ile anlaşabilir. Bu durumda, kişisel veriler bu konuda uzman olan kişi tarafından bir daha kurtarılamayacak biçimde güvenli olarak silinir/yok edilir.

11.4 Kişisel Verileri Anonim Hale Getirme Teknikleri

11.4.1 Kişisel verilerin anonimleştirilmesi, kişisel verilerin başka verilerle eşleştirilerek dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder. Şirket, hukuka uygun olarak işlenen kişisel verilerin işlenmesini gerektiren sebepler ortadan kalktığında kişisel verileri anonimleştirebilmektedir.

11.4.2 KVK Kanunu'nun 28. maddesine uygun olarak; anonim hale getirilmiş olan kişisel veriler araştırma, planlama ve istatistik gibi amaçlarla işlenebilir. Bu tür işlemeler KVK Kanunu kapsamı dışındadır. Anonim hale getirilerek işlenen kişisel veriler KVK Kanunu kapsamı dışında olacağından politikanın 10. bölümünde düzenlenen haklar bu veriler için geçerli olmayacaktır.

11.4.3 Maskeleme (Masking) Veri maskeleme, kişisel verinin temel belirleyici bilgisini veri seti içerisinden çıkartılarak kişisel verinin anonim hale getirilmesi yöntemidir. Örnek: Kişisel veri sahibinin tanımlanmasını sağlayan isim, TC Kimlik No, ad, soyad vb. bilginin çıkartılması yoluyla kişisel veri sahibinin tanımlanmasının imkansız hale geldiği bir veri setine dönüştürülmesi.

11.4.4 Toplulaştırma (Aggregation) Veri toplulaştırma yöntemi ile birçok veri toplulaştırılmakta ve kişisel veriler herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmektedir. Örnek: Müşterilerin doğum yıllarını tek tek göstermeksizin 1975 yılında doğan 100 müşteri bulunduğunun ortaya konulması.

11.4.5 Veri Türetme (Data Derivation) Veri türetme yöntemi ile kişisel verinin içeriğinden daha genel bir içerik oluşturulmakta ve kişisel verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesi sağlanmaktadır. Örnek: Doğum tarihleri yerine yaşların belirtilmesi; açık adres yerine ikamet edilen ilçenin veya şehirin belirtilmesi.

11.4.6 Veri Karma (Data Shuffling, Permutation) Veri karma yöntemi ile kişisel veri seti içindeki değerlerinin karıştırılarak değerler ile kişiler arasındaki bağın kopartılması sağlanmaktadır. Örnek: Ses kayıtlarının niteliğinin değiştirilerek sesler ile veri sahibi kişinin ilişkilendirilemeyecek veya tanınamayacak hale getirilmesi.

12. Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimleri ve görev tanımları:

12.1. ***Bilgi İşlem Birimi Yöneticisi;*** Şirketin tüm Bilgi İşlem süreçlerini yönetir.

12.2. ***İnsan Kaynakları Yöneticisi*** *(Personel ile ilgili konularda)*, Şirketin tüm personel süreçlerini yönetir.

12.3. ***Satış ve Pazarlama Yöneticisi*** *(Müşteri bilgileri ile ilgili konularda);* Şirketin tüm satış pazarlama süreçlerini yönetir.

13. Saklama ve imha sürelerini gösteren tablo

NO	VERİ KATEGORİSİ	VERİ SAKLAMA SÜRESİ
1	Kimlik	10 YIL
2	İletişim	10 YIL
3	Lokasyon	2 YIL
4	Özlük	10 YIL
5	Hukuki İşlem	10 YIL

6	Müşteri İşlem	10 YIL
7	Fiziksel Mekân Güvenliği	2 YIL
8	İşlem Güvenliği	10 YIL
9	Risk Yönetimi	10 YIL
10	Finans	10 YIL
11	Mesleki Deneyim	10 YIL
12	Pazarlama	10 YIL
13	Görsel ve İşitsel Kayıtlar	10 YIL
14	Kılık ve Kıyafet	10 YIL
15	Sağlık Bilgileri	10 YIL
16	Ceza Mahkûmiyeti Ve Güvenlik Tedbirleri	10 YIL
17	Dernek Üyeliği	10 YIL
18	Biyometrik Veri	5 YIL

14. Periyodik imha süreleri,

14.1. Şirket saklama süresi dolan kişisel verileri saklama süresinin dolduğu tarihten itibaren en geç 180 gün içerisinde imha eder.

14.2. Şirket; kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

14.3. Periyodik imhanın gerçekleştirileceği zaman aralığı veri sorumlusu tarafından kişisel veri saklama ve imha politikasına, prosedürlere ve şirketin iş akışına uygun olarak belirlenir. Bu süre her halde altı ayı geçemez.

15. Politikanın Yayınlanması ve Saklanması

Politika, ıslak imzalı (basılı kâğıt) ve elektronik ortamda olmak üzere iki farklı ortamda yayımlanır, internet sayfasında kamuya açıklanır.

16. Güncelleme Periyodu

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

17. Yürürlük

Politika, Şirketin internet sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.