

	<b>KİŞİSEL VERİLERİN KORUNMASI</b>	Versiyon	<b>1.1</b>
		İlk Yayın Tarihi	
	Kişisel Verilerin Saklanması ve İmhası Politikası	Son Güncelleme Tarihi	<b>17.05.2021</b>
		Sayfa No	<b>1 / 33</b>

**B-PLAS BURSA PLASTİK METAL İNŞAAT ENERJİ MADENCİLİK JEOTERMAL TURİZM SİVİL**

**HAVACILIK VE TARIM SANAYİ VE TİCARET ANONİM ŞİRKETİ**

**KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI POLİTİKASI**

**İÇİNDEKİLER**

1. GİRİŞ.....	2
2. AMAÇ VE KAPSAM .....	3
3. TANIMLAR.....	3
4. POLİTİKA İLE DÜZENLEME ALTINA ALINAN KAYIT ORTAMLARI.....	6
5. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASINI GEREKTİREN HUKUKİ, TEKNİK VE DİĞER SEBEPLER.....	6
5.1. Kişisel Verilerin Saklanmasına İlişkin Açıklamalar .....	7
5.1.1. Saklamayı Gerektiren Hukuki Sebepler.....	7
5.1.2. Saklamayı Gerektiren İşleme Amaçları .....	8
5.2. Kişisel Verilerin İmhasına İlişkin Açıklamalar.....	9
6. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER .....	10
6.1. İdari Tedbirler.....	10
6.2. Teknik Tedbirler.....	12
6.3. Özel Nitelikli Kişisel Verilerin Saklanması.....	14
6.4. Kişisel Verilerin Saklanmasına İlişkin Diğer Teknik Uygulama ve Tedbirler .....	15
7. KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER .....	16
7.1. Kişisel Verilerin Silinmesi.....	16
7.1.1. Kağıt Ortamında Bulunan Kişisel Veriler .....	17
7.1.2. Merkezi Sunucuda Yer Alan Ofis Dosyaları .....	17
7.1.3. Taşınabilir Medyada Bulunan Kişisel Veriler.....	17
7.1.4. Veri Tabanları.....	17
7.2. Kişisel Verilerin Yok Edilmesi.....	17
7.2.1. Yerel Sistemler .....	18
7.2.2. Çevresel Sistemler.....	18

7.2.3. Kağıt Ortamlar.....	18
7.3. Kişisel Verilerin Anonim Hale Getirilmesi.....	19
7.3.1. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri.....	19
7.3.2. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri.....	21
7.3.3. Anonimlik Güvencesi.....	23
8. KİŞİSEL VERİ SAKLAMA VE İMHA SÜREÇLERİNDE GÖREV VE SORUMLULUK DAĞILIMLARI	23
9. SAKLAMA VE İMHA SÜRELERİ TABLOSU .....	26
10. PERİYODİK İMHA SÜRESİ.....	31
11. İLGİLİ KİŞİNİN TALEBİ ÜZERİNE SİLME VE YOK ETME SÜRELERİ.....	32
12. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI POLİTİKASINDA YAPILACAK GÜNCELLEMELER	32
13. YÜRÜRLÜK.....	33

## 1. GİRİŞ

Günümüzde binlerce gerçek kişiye ilişkin bilgilere gerek devlet kurumları gerekse özel kuruluşlar tarafından kolaylıkla erişilebilmektedir. Bilişim teknolojilerindeki gelişmeler ve dijital çağın getirileri doğrultusunda kişisel verilerin korunması ihtiyacı gittikçe artmıştır.

Bu doğrultuda 1970’li yıllardan bu yana, ulusal ve uluslararası düzenlemeler ile kişisel verilerin korunmasına yönelik çalışmalar yürütülmektedir. Ülkemizde 2010 yılında 5982 sayılı Kanunla Anayasanın 20.maddesine eklenen fıkra ile kişisel verilerin korunmasını isteme hakkı anayasal bir hak olarak teminat altına alınmıştır. Bu kapsamda ve Türk Ceza Kanunu’nda yapılan düzenlemelerin de ardından, taslak halinde olan 6698 sayılı Kişisel Verilerin Korunması Kanunu (“KVKK” ya da “KVK Kanunu”) Türkiye Cumhuriyeti Büyük Millet Meclisi tarafından kabul edilmiş ve 7 Nisan 2016 tarih ve 29677 sayılı Resmi Gazete’de yayımlanarak yürürlüğe girmiştir.

B-PLAS Bursa Plastik Metal İnşaat Enerji Madencilik Jeotermal Turizm Sivil Havacılık ve Tarım Sanayi ve Ticaret Anonim Şirketi hukuka, kanuna ve yasal düzenlemelere uyumlu hareket etmeyi benimsemiş bir şirket olarak KVK Kanununa da doğan yükümlülüklerini yerine getirerek kişisel verilerin korunması ve güvenliğinin sağlanması adına gerekli adımları atmıştır. Bu kapsamda kapsamında kişisel verilerin korunmasına ilişkin tedbirler uygulamaya geçirilmiş ve işbu Kişisel Verilerin Saklanması ve İmhası Politikası, B-PLAS Bursa Plastik Metal İnşaat

Enerji Madencilik Jeotermal Turizm Sivil Havacılık ve Tarım Sanayi ve Ticaret Anonim Şirketi tarafından yürürlüğe konulmuştur.

## 2. AMAÇ VE KAPSAM

İşbu Kişisel Verilerin Saklanması ve İmhası Politikasının (“Saklama ve İmha Politikası”) amacı; B-PLAS Bursa Plastik Metal İnşaat Enerji Madencilik Jeotermal Turizm Sivil Havacılık ve Tarım Sanayi ve Ticaret Anonim Şirketi (“Şirket”) tarafından tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollar ile 6698 sayılı Kişisel Verilerin Korunması Kanununa ve diğer ilgili yasal mevzuatlara uygun olarak işlenen kişisel verilerin işlendikleri amaç için olan azami sürelerinin belirlenmesi ve Şirket tarafından uygulanan saklama ve imha faaliyetlerine ilişkin usul ve esasların belirlenmesidir.

İşbu Saklama ve İmha Politikası’nda, 28 Ekim 2017 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi hakkındaki Yönetmeliğin (“Yönetmelik”) 6’ncı maddesinde yer alan veri güvenliğini sağlamak için alınmış teknik ve idari tedbirlere de yer verilmektedir.

B-PLAS Bursa Plastik Metal İnşaat Enerji Madencilik Jeotermal Turizm Sivil Havacılık ve Tarım Sanayi ve Ticaret Anonim Şirketi, Veri Sorumlusu olarak çalışan adaylarının, çalışanlarının, tedarikçilerinin, müşterilerinin ve ziyaretçilerinin kişisel verilerini elektronik ve elektronik olmayan kayıt ortamlarında saklanmasında ve söz konusu işleme sebeplerinin ortadan kalktığında kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirmesinde işbu Politikayı uygulamaktadır.

## 3. TANIMLAR

<b>Açık Rıza</b>	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
<b>Alıcı Grubu</b>	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.
<b>Anonim Hale Getirme</b>	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi.

<b>İlgili Kişi/Veri Sahibi</b>	Kişisel verisi işlenen gerçek kişi.
<b>İlgili Kullanıcı</b>	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen gerçek veya tüzel kişilerdir.
<b>KVKK/KVK Kanunu</b>	6698 Sayılı Kişisel Verilerin Korunması Kanunu.
<b>Karartma</b>	Kişisel verilerin bütünü, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işlemleri ifade etmektedir.
<b>Kayıt Ortamı</b>	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.
<b>Kişisel Veri</b>	Kimliği belirli veya belirlenebilir gerçek kişiyle eşleştirilebilen her türlü bilgi.
<b>Kişisel Verilerin İmhası</b>	Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi.
<b>Kişisel Veri İşleme Envanteri</b>	Veri sorumlusu olarak iş süreçlerine bağlı olarak gerçekleştirmekte olduğumuz kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğumuz ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri detaylandıran envanterimiz.

<b>Kişisel Verilerin İşlenmesi</b>	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.
<b>Kişisel Verilerin Silinmesi</b>	Kişisel Verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi.
<b>Kişisel Verilerin Yok Edilmesi</b>	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.
<b>KVK Kurulu</b>	Kişisel Verileri Koruma Kurulu.
<b>KVK Kurumu</b>	Kişisel Verileri Koruma Kurumu
<b>Maskeleme</b>	Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemleri ifade etmektedir.
<b>Özel Nitelikli Kişisel Veri</b>	Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri. Politikada aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel veriler birlikte "Kişisel Veriler" olarak adlandırılacaktır.
<b>Periyodik İmha</b>	Kanun'da yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi.

<b>Veri İşleyen</b>	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.
<b>Veri Kayıt Sistemi</b>	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi.
<b>Veri Sorumlusu</b>	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.

İşbu Saklama ve İmha Politikasında yer almayan tanımlar için KVK Kanunu'nda belirtilen tanımlar geçerlidir.

#### 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 olarak adlandırılmaktadır. Bu ortamlar genel olarak aşağıdaki gibidir;

- **Fiziki Ortamlar:** Kişisel Verilerin kağıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır (*örneğin: kağıtlar, matbu yazılı formlar, anket formları, ziyaretçi giriş-çıkış defterleri, basılı ve görsel ortamlar*);
- **Yerel dijital ortamlar:** Şirket bünyesinde yer alan bilgisayarlar, sunucular, sabit ya da taşınabilir diskler, *örneğin: e-posta, veri tabanı, kişisel bilgisayarlar, mobil cihazlar, USB, hafıza kartı, yazıcı, tarayıcı, fotokopi makinesi, güvenlik duvarı, antivirüs*);optik diskler gibi sair dijital ortamlardır (
- **Bulut ortamlar:** Şirket bünyesinde yer almamakla birlikte, Şirket'in kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.

Şirket faaliyetleri esnasında işlediği Kişisel Verileri fiziki ve yerel dijital ortamlarda hukuka uygun ve güvenli olarak saklamaktadır.

#### 5. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASINI GEREKTİREN HUKUKİ, TEKNİK VE DİĞER SEBEPLER

B-PLAS Bursa Plastik Metal İnşaat Enerji Madencilik Jeotermal Turizm Sivil Havacılık ve Tarım Sanayi ve Ticaret Anonim Şirketi bünyesinde yer alan departmanlar iş tanımları kapsamında

yürütülen iş süreçleri ve işbu süreçlere bağlı faaliyetleri gerçekleştirebilmek amacıyla çalışanlarının, çalışan adaylarının, tedarikçilerinin, müşterilerinin ve ziyaretçilerinin olmak üzere farklı ilgili kişi kategorilerine ait kişisel verileri KVK Kanununa ve ilgili yasal mevzuata uygun olarak işlemektedir.

Bu doğrultuda kişisel verilerin saklanması ve imhasına gerektiren hukuki, teknik ve diğer sebeplere ilişkin detaylı açıklama aşağıda yer almaktadır.

### **5.1. Kişisel Verilerin Saklanması İlişkin Açıklamalar**

KVK Kanununun 4. maddesinde kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve *“İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi”* demek suretiyle kişisel verilerin işlenmesi amaç ve süre yönüyle sınırlandırılmıştır. Bu kapsamda ve KVK Kanununun 5 maddesinde yer alan işleme şartlarına uygun olarak, kişisel veriler hukuki sebepler ile uyumlu olarak ve mevzuatta öngörülen veya Şirket tarafından kişisel veri işleme amacı çerçevesinde belirlenen süreler boyunca saklanmaktadır.

#### **5.1.1. Saklamayı Gerektiren Hukuki Sebepler**

Şirket tarafından işlenen kişisel verilerin saklanmasını gerektiren hukuki sebepler sıradaki gibidir:

- a) Şirket faaliyetlerinin yerine getirilmesi uyarınca, İlgili Kişilerin açık rızasının alınmasını gerektiren saklama faaliyetleri açısından İlgili Kişinin açık rızasının bulunması,
- b) Kişisel Verilerin işlenmesi ilgili kanunlarda ve mevzuatlarda açıkça öngörülmesi; Şirket faaliyetleri esnasında işlediği kişisel verileri sıradaki Kanunlarda öngörülen süreler zarfında saklamaktadır:

- 6098 sayılı Türk Borçlar Kanunu,
- 4857 sayılı İş Kanunu,
- 6331 sayılı İş Sağlığı ve Güvenliği Kanunu,
- 6102 sayılı Türk Ticaret Kanunu,
- 6356 sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu ve İlgili Mevzuat,
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- Avukatlık Kanunu ve İlgili Mevzuat,

- 213 sayılı Vergi Usul Kanunu,
  - 5434 sayılı Emekli Sağlığı Kanunu,
  - 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
  - 4982 Sayılı Bilgi Edinme Kanunu,
  - İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
  - Arşiv Hizmetleri Hakkında Yönetmelik
- c) Kişisel verilerin sözleşmelerin kurulması ve ifası ile doğrudan doğruya ilgili olması,
- d) Şirket faaliyetleri uyarınca temas halinde olunan İlgili Kişilerin, fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunması veya rızasına hukuki geçerlik tanınmaması sebebiyle, kendisinin veya bir başkasının hayatı ve beden bütünlüğünün korunabilmesi için saklanmasının zorunlu olması,
- e) Kişisel verilerin Şirket'in yerine getirmekte olduğu faaliyetler kapsamında hukuki yükümlülüğünü yerine getirmesi,
- f) Şirket tarafından yürütülen faaliyetler ile uyumlu olarak, İlgili Kişinin kendisi tarafından alenileştirilmesi,
- g) Kişisel verilerin bir hakkın tesisi, kullanılması veya korunması amacıyla saklanması,
- h) Kişisel verilerin kişilerin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirket'in meşru menfaatleri için saklanması

### 5.1.2. Saklamayı Gerektiren İşleme Amaçları

Şirket, faaliyetleri esnasında işlediği kişisel verileri işbu verilerin işleme amacına bağlantılı, sınırlı ve ölçülü olarak aşağıda örnek niteliğinde yer verilen ve Kişisel Veri İşleme Envanterinde detaylandıran işleme amaçları kapsamında belirli sürelerle saklamaktadır.

- a) Acil Durum Süreçlerinin Yürütülmesi,
- b) Bilgi Güvenliği Süreçlerinin Yürütülmesi,
- c) Finansal ve muhasebe işlemlerinin yürütülmesi,
- d) Mevzuattan kaynaklanan hukuki yükümlülüklerin yerine getirilmesi,
- e) Hukuki süreçlerin takibi,
- f) İnsan kaynakları süreçlerinin planlanması ve icrası,
- g) İletişim faaliyetlerinin planlanması ve icrası,
- h) Mal/hizmet satış, satın alım ve müşteri ilişkilerinin yürütülmesi,



- i) Sözleşmelerin kurulması ve/veya ifası,
- j) Şirket ve çalışanlarının güvenliğinin temini,
- k) Yönetim faaliyetlerinin yürütülmesi.

## 5.2. Kişisel Verilerin İmhasına İlişkin Açıklamalar

İlgili saklama süreleri sona erdiğinde veya işleme amacı ortadan kalktığına, kişisel veriler işbu Politika'da belirlenen silme, yok etme veya anonim hale getirme yöntemleri ile aşağıdaki sebeplerle Şirket tarafından re'sen veya ilgili kişinin talebi üzerine imha edilir;

- a) İlgili Kişinin açık rıza şartına bağlı olarak işlenerek saklanmakta olan Kişisel Veriler, İlgili Kişinin rızasını geri alması halinde,
- b) Kişisel verilerin işlenmesine veya saklanmasına esas teşkil eden ilgili mevzuat hükümlerinin değişmesi veya ilgası,
- c) Kişisel verilerin işlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- d) Taraflar arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,
- e) Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olduğunun tespit edilmesi,
- f) Kanun'un 5. ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,
- g) İlgili kişinin, KVK Kanunu madde 11/1(e) ve (f) bentlerindeki hakları çerçevesinde kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin yaptığı başvurunun veri sorumlusu olarak Şirket tarafından kabul edilmesi,
- h) Şirket'in, İlgili Kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, Şirketin verdiği cevabın İlgili Kişi tarafından yetersiz bulunması veya Şirket'in KVK Kanunu'nda öngörülen süre içinde cevap vermemesi hallerinde; İlgili Kişinin KVK Kurulu'na şikâyetinde bulunulması ve bu talebin KVK Kurulu tarafından uygun bulunması,
- i) Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

## 6. KİŞİSEL VERİLERİN GÜVENLİ BİR ŞEKİLDE SAKLANMASI İLE HUKUKA AYKIRI OLARAK İŞLENMESİ VE ERİŞİLMESİNİN ÖNLENMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER

KVK Kanununun 12. maddesinin birinci fıkrasında; Veri Sorumlusu'nun; "a) *Kişisel Verilerin hukuka aykırı olarak işlenmesini önlemek, b) Kişisel Verilere hukuka aykırı olarak erişilmesini önlemek, c) Kişisel Verilerin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır* " demek suretiyle Veri sorumlusunun kişisel verilerin güvenliğine ilişkin yükümlülükleri düzenlenmiştir.

Şirket, işbu veri güvenliği yükümlülüğü ve KVK Kanununun 6. Maddesi 4. Fıkrasında öngörülen özel nitelikli kişisel verilerin işlenmesinde Kurul tarafından belirtilen yeterli önlemleri alarak faaliyetleri kapsamında ve işbu politikada belirtilen sebeplerle saklanmakta olan Kişisel veriler ve özel nitelikli kişisel veriler için başlıca aşağıdaki idari ve teknik tedbirleri uygulamaktadır.

### 6.1. İdari Tedbirler

Şirket tarafından uygulanan idari tedbirler sıradaki gibidir:

- a) **Mevcut risk ve tehditlerin belirlenmesi:** Şirket tarafından Kişisel Veri İşleme Envanteri hazırlanarak, işlenen kişisel verilerin kategorileri, işleme amacı, aktarıldığı alıcı grupları, saklama süreleri, verisi işlenen ilgili kişi grubu belirlenerek kişisel verilere ilişkin süreç ortaya çıkarılarak alınması gereken tedbirler belirlenmiştir.
- b) **Aydınlatma yükümlülüğünün yerine getirilmesi:** kişisel veri işleme faaliyetlerine başlanmadan önce ilgili kişilere kategori bazında hazırlanmış olan aydınlatma metinleri sunulmaktadır.
- c) **Çalışanların eğitilmesi ve farkındalık çalışmaları:** Kişisel verilerin korunmasına ilişkin kurum kültürünün oluşturulabilmesi için KVK Kanununda yer alan önemli terim ve kavramları, kişisel verilerin korunmasının önemi, bilgi güvenliği ve gizlilik konularında şirket çalışanlarına eğitimler verilmektedir. Temel eğitim ve farkındalık çalışmalarının yanı sıra, kişisel verilerin işlenmesine ilişkin politikaların değişmesi halinde, yeni politikalara uyum sağlamak amacıyla verilen eğitimler tekrarlanmaktadır.
- d) **Kişisel verilerin güvenliğine ilişkin politikalara uyumun sağlanması:** KVK Kanunu kapsamında veri sorumlusu sıfatıyla Şirket olarak hazırlamakla yükümlü olduğumuz politikaların yanı sıra çalışanlarına yönelik gizlilik sözleşmeleri imzalatılmakta ve iç etik kuralları, iç yönerge, bilgi güvenliği politikası gibi metinler kanun kapsamında revize edilerek uyulması gereken usul ve yasaklar hakkında çalışanlar bilgilendirilmektedir.
- e) **Disiplin Prosedürü:** Kişisel verilerin korunması eğitim ve farkındalıklara katılmayan, kişisel verilerin güvenliğine ve korunmasına yönelik belirlenen kural, usul, prensip ve yükümlülüklerine aykırı hareket eden çalışanlara yönelik uygulanacak disiplin prosedürü hazırlanmıştır.

- f) **Minimum veri işleme:** Veri Sorumlusu sıfatıyla Şirket'in kişisel veri işleme amaçları çerçevesinde en az sayıda veri işleme sağlanmakta ve işleme ihtiyacı duyulmayan veriler de kişisel veri saklama ve imha politikası uyarınca silinmekte, yok edilmekte ya da anonim hale getirilmektedir.
- g) **Veri işleyenlerle ilişkilerin yönetimi:** KVK Kanunu'nun 12/II. Maddesi uyarınca kişisel verilerin güvenliğinin sağlanması noktasında veri işleyenlerden de gerekli taahhütler alınmakta, iş ilişkisi içerisinde bulunan iş ortaklarımız, tedarikçilerimiz, çözüm ortaklarımız ile kişisel verilerin işlenmesine, muhafazasına ilişkin protokoller imzalanarak, Şirket tarafından KVK Kanunu madde 5'te yer alan hukuki sebeplerle işlenen ve 3.kişilere aktarılan verilerin muhafazası ve güvenliği sağlanmaktadır.
- h) **Kişisel verilerin işlenmesi prosedürlerinin yönetimi:** Saklanan kişisel verilere erişim iş tanımı gereği erişmesi gerekli personel ile sınırlandırılmaktadır. Kişisel verilerin işlenmesi, muhafazası, imhasına ilişkin süreçlerin takibi, kişisel verilere ilişkin Şirkete iletilen taleplerin yönetimi için Şirket içerisinde görevlendirmeler yapılmaktadır. Kişisel verilere ilişkin süreçlerin KVK Kanunu'na uygun olarak yerine getirilmesi için profesyonel danışmanlık alınmaktadır.
- i) **Kişisel verilerin işlenmesi ve güvenliğine ilişkin denetimler:** Şirket, KVK Kanunu hükümlerinin uygulanmasını sağlamak amacıyla gerekli periyodik ve rastgele iç denetimleri yapmaktadır.
- j) **Kişisel verilerin saklanmasına ilişkin diğer idari uygulama ve tedbirler:** İşlenen Kişisel Verilerin güvenliğinin sağlanması amacıyla Şirket bünyesinde yukarıda belirtilenlere ek olarak, genel olarak aşağıdaki idari tedbirler uygulanmaktadır;
- Çalışanlar İçin Disiplin Düzenlemeleri;
  - Çalışanlara Verilen Eğitim ve Farkındalık Çalışmaları
  - Çalışanlar İçin Yetki Matrisleri
  - Çalışanların Erişim Yetkilerinin Gerektiğinde Güncellenmesi
  - Erişim, Bilgi Güvenliği, Saklama, Kullanım, İmha Politikaların Oluşturulması
  - Gizlilik Taahhütnamelerinin Alınması
  - Sözleşmelerde Veri Güvenliğine İlişkin Hükümlerin Eklenmesi
  - Kişisel Veri Güvenliği, Politika ve Prosedürlerin Belirlenmesi
  - Kişisel Veri Güvenliğine İlişkin Sorunların Takibi ve Raporlanması
  - Kişisel Verilerin Minimuma Azaltılması
  - Kanun İçi Periyodik Güncellemelerin Yapılması
  - Mevcut Risk ve Tehdit Kontrolleri
  - Özel Nitelikli Kişisel Verilere İlişkin Politika ve Prosedürlerin Uygulanması

- Veri İşleyen Hizmet Sağlayıcının Veri Güvenliği Konusunda Farkındalığı sağlanmaktadır;

## 6.2. Teknik Tedbirler

Şirket tarafından alınan teknik tedbirler sıradaki gibidir:

- a) Siber Güvenliğin Sağlanması:** Kişisel Veri Güvenliğinin Sağlanması amacıyla siber güvenlik sistemleri kurulmuştur ve güncelliği sağlanmaktadır. Bu kapsamda;
- İnternet üzerinden gelen izinsiz erişim tehditlerine karşı alınabilecek öncelikli tedbirler olarak güvenlik duvarı ve internet ağ geçidi kullanılmaktadır,
  - Kullanılmayan yazılım ve servisler kaldırılarak yazılımların eski sürümlerinin güvenlik açıkları içermesi ihtimaline karşılık bu yazılım ve servislerin güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikle tercih edilebilecek bir yöntemdir,
  - Özellikle kişisel verilerin yer aldığı sistemlerin yönetilmesi amacıyla dışarıdan temin edilen yazılımların ve modüllerinin güncelliğinin takibinin sağlanması amacıyla yama yönetimi ve yazılım güncellemeleri gerçekleştirilerek olası güvenlik açıklarının kapatılması sağlanmaktadır.
- b) Yetki matris ve kontrolü:** Kişisel veri içeren sistemlere erişim sağlayacak personelin görev tanımıyla uyumlu olarak sınırlandırılmıştır.
- Özellikle Şirket çalışanlarının elektronik ve fiziki ortamlarda kişisel verilere erişim yetkilerinin kontrol altında tutulmasını sağlanmaktadır.
  - Kaba kuvvet algoritması (BFA) kullanımı gibi yaygın saldırılardan korunmak için şifre girişi deneme sayısının sınırlandırılması, düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması, yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması ve veri sorumlusuyla ilişkileri kesilen çalışanlar için zaman kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması gibi yöntemlerle de erişim sınırlandırılmaktadır.
  - Yetki matris ve kontrol sistemi kapsamında kullanıcıların hem sisteme giriş çıkışlarının hem de etkinlik kayıtlarının (log) düzenli olarak tutulması da geçmişe yönelik siber risklerin tespiti ve incelenmesi açısından önem arz etmektedir.
- c) Şifre ve Parolaların Oluşturulmasına ilişkin önlemlerin belirlenmesi:** Şirket çalışanları tarafından kullanılan şifre ve parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesi sağlanmaktadır.

- d) Güncel anti-virüs yazılımlarının kullanılması:** Kötü amaçlı yazılımlardan korunmak için bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden anti-virüs, anti-spam gibi ürünler kullanılmaktadır. Ancak bu ürünlerin sadece kurulumunun yeterli olmaması sebebiyle güncelliklerinin sağlanmasına da dikkat edilerek gerekli virüs taramaları düzenli olarak yapılmaktadır.
- e) Veri aktarımlarında SSL protokolünün kullanılması:** Veri sorumluları tarafından, farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL, sFTP ya da diğer güvenli yollar ile gerçekleştirilmesine riayet edilmektedir.
- f) Güvenlik problemlerine ilişkin raporlama sisteminin kurulması:** Bilişim sistemlerinin bilinen zafiyetlere karşı korunması için düzenli olarak *zafiyet taramaları* ve *sızma testlerinin* yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılmaktadır.
- g) Kişisel Veri İçeren Ortamların Güvenliğinin sağlanması:** kişisel veri içeren ortamlar tespit edilerek, saklanan kişisel verilerin güvenliğinin alınması ve verilere izinsiz erişimin engellenmesi amacıyla farklı ortamlara ilişkin tedbirler alınmaktadır.
- h) Şirket yerleşkelerinde kâğıt ortamında saklanan veriler:** kâğıtların çalınması veya kaybolması gibi tehditlere karşı dolap ve çekmecelerin kilit altına alınması gibi fiziksel güvenlik önlemler alınmaktadır. Kişisel verilerin yer aldığı fiziksel ortamların dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunması ve bu ortamlara giriş / çıkışların kontrol altına alınmasına dikkat edilmektedir.
- i) Elektronik ortamda saklanan Kişisel Veriler:** kişisel veri güvenliği ihlalini önlemek için ağ bileşenleri arasında erişim sınırlandırılmaktadır. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil de sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılacaktır.
- j) Çalışanların şahsi elektronik cihazlarının bilgi sistem ağına erişiminin sınırlandırılması:** Çalışanların şahsi elektronik cihazlarının, bilgi sistem ağına erişim sağlaması da güvenlik ihlali riskini arttırdığından bu cihazlara bilgi sistem ağına erişim hakkı verilmemektedir.
- k) Fiziki tedbirler:** Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kâğıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınması (arşiv odası), kullanılmadığı zaman kilit altında tutulması, giriş çıkış kayıtlarının tutulması gibi fiziksel güvenliğin arttırılmasına ilişkin önlemler alınmaktadır.

- l) Email/Bilgisayar ortamında saklanan kişisel veriler:** Çalışanlara atanan e-mail ve bilgisayarlarda saklanan kişisel verilerin minimuma indirilmesi için çalışanlar bilgilendirilmekte ve cihazların dışarıdan gelecek saldırılara karşı güvenliği sağlanmaktadır.
- m) Bilgi Teknolojileri sistemleri tedarigi, geliştirmesi ve bakımı:** Kişisel veri içeren cihaz/sistemlerin bakımının dış kaynaklı hizmetler (üretici, satıcı, servis gibi üçüncü kurumlar) tarafından gerçekleştirilecek olması durumunda kişisel verilerin güvenliğinin sağlanması için cihazlardaki veri saklama ortamlarının sökülerek bakıma gönderilmesi sağlanmaktadır. Bakım ve onarım gibi amaçlarla dışarıdan personel gelmişse kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir. Belirtilen amaçlarla dışarıdan hizmet alınması durumunda, veri güvenliğinin sağlanması amacıyla hizmet alınan şirketlerin tamamıyla KVK Kanunu m. 12/II'den kaynaklanan yükümlülüklerin yerine getirilmesi amacıyla, şirketlerle yapılan mevcut sözleşmeler veri güvenliğine ilişkin hükümler içerecek şekilde revize edilmektedir.
- n) Kişisel Verilerin Yedeklenmesi:** Kişisel veriler içeren ortamlar belirli periyotlarla yedeklemek suretiyle güvenlik altına alınmaktadır. Bu kapsamda, yedekleme stratejilerinin oluşturulmakta ve veri seti yedeklerinin ağ dışında tutulması sağlanmaktadır.

### 6.3. Özel Nitelikli Kişisel Verilerin Saklanması

KVK Kurulu tarafından yayımlanan "*Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler*" ile ilgili 31/01/2018 Tarihli ve 2018/10 Sayılı Karar uyarınca veri Sorumlusu olarak Şirketimiz, işlenen özel nitelikli kişisel verilerin saklanmasında yukarıda detaylandırılan diğer önlemlerle birlikte ayrıca aşağıda belirlenmiş güvenlik önlemlerinin alınmasını sağlamaktadır;

- a) Çalışanlar İçin Yetki Matrisleri oluşturulmaktadır;
- b) Özel nitelikli kişisel veriler ile temas eden çalışanlara yönelik özel nitelikli kişisel verilerin güvenliği ve önemi hususunda eğitimler verilmiş, gizlilik sözleşmeleri imzalanmış ve erişim sınırlandırılmaları getirilmiştir;
- c) Erişim Loglarının Düzenli Olarak Tutulması;
- d) Özel nitelikli kişisel verilerin bulunduğu ortamlara fiziksel güvenlik önlemleri alınmış olup yetkisiz kişilerin erişimi engellenmiştir;
- e) Özel nitelikli kişisel verilerin bulunduğu/muhafaza edildiği dijital ortamlar kilitlenmiş, kodlanmış veya şifrelenmiş sistem girişleri kullanılmaktadır;
- f) Log Kayıtlarının Kullanıcı Müdahalesinden Korunması Sağlanmaktadır;
- g) Özel Nitelikli Kişisel Veriler İçin güvenli şifreleme / kriptografik anahtarlar kullanılmaktadır
- h) Uzaktan erişimin gerektiği verilere, iki kademeli kimlik doğrulama sistemiyle erişim sağlanmaktadır;

- i) Verilerin bulunduğu ortamlara ait yazılımlarda güvenlik güncellemeleri takip edilmektedir;
- j) Özel nitelikli kişisel verilere yönelik yedekleme/kademeli Kimlik Doğrulama uygulanmaktadır.

#### 6.4. Kişisel Verilerin Saklanması İlişkin Diğer Teknik Uygulama ve Tedbirler

İşlenen Kişisel Verilerin güvenliğinin sağlanması amacıyla Şirket bünyesinde yukarıda belirtilen önlemlere ek olarak, genel olarak aşağıdaki teknik tedbirler uygulanmaktadır:

- a) Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
- b) Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- c) Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
- d) Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- e) Gizlilik taahhütnameleri yapılmaktadır.
- f) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- g) Güncel anti-virüs sistemleri kullanılmaktadır.
- h) Güvenlik duvarları kullanılmaktadır.
- i) İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- j) Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- k) Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
- l) Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- m) Kişisel veri güvenliğinin takibi yapılmaktadır.
- n) Kişisel veri içeren fiziksel ortamlara giriş çıkışlarla ilgili gerekli güvenlik önlemleri alınmaktadır.
- o) Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
- p) Kişisel veri içeren ortamların güvenliği sağlanmaktadır.
- q) Kişisel veriler mümkün olduğunca azaltılmaktadır.
- r) Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
- s) Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- t) Kurum içi periyodik ve/veya rastgele denetimler yapılmakta ve yaptırılmaktadır.
- u) Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- v) Mevcut risk ve tehditler belirlenmiştir.

- w) Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
- x) Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- y) Şifreleme yapılmaktadır.
- z) Veri işleyen hizmet sağlayıcılarının, veri güvenliği konusunda farkındalığı sağlanmaktadır

## **7. KİŞİSEL VERİLERİN HUKUKA UYGUN OLARAK İMHA EDİLMESİ İÇİN ALINMIŞ TEKNİK VE İDARİ TEDBİRLER**

KVK Kanunu 7. maddesi uyarınca mevzuatta öngörülen sürelerin dolması veya kişisel verilerin işleme amacı için gerekli sürelerin sonunda, kişisel veriler KVK Kanunu'nun 4. Maddesinde öngörülen ilkeler ve Kanunu'nun 12. Maddesi kapsamında alınması gereken teknik ve idari tedbirle, ilgili mevzuat hükümlerine, KVK Kurulu kararlarına ve Şirketimiz tarafından hazırlanan işbu Kişisel Verilerin Saklanması ve İmhası Politikası'nda belirtilen esaslara uygun olarak aşağıda açıklanacak yöntemlerle silinmekte, yok edilmekte veya anonim hale getirilmektedir.

### **7.1. Kişisel Verilerin Silinmesi**

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu olarak Şirketimiz silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli teknik ve idari tedbirleri almaktadır.

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri işleme amacı için ilgili kullanıcıların tespit edilmesi
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi
- İlgili kullanıcıların kişisel veriler kapsamında erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması

Bu madde altında belirtilen yöntemler yönetmelik ve rehberde yer almakta olup, kişisel verilerin silinmesinde seçilecek yöntem Şirketimizin iç prosedürleri kapsamında ilgili olduğu ölçüde aşağıdaki tedbirler seçilmek suretiyle uygulanmaktadır.



### **7.1.1. Kağıt Ortamında Bulunan Kişisel Veriler**

Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinmektedir. Karatma işlemi ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemeyecek ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak ilgili kullanıcılara görünemez hale getirilmesi şeklinde yapılmaktadır.

### **7.1.2. Merkezi Sunucuda Yer Alan Ofis Dosyaları**

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması suretiyle işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilerek silme işlemi gerçekleştirilir.

### **7.1.3. Taşınabilir Medyada Bulunan Kişisel Veriler**

Flash tabanlı saklama ortamlarındaki kişisel veriler sistem yöneticisi tarafından şifreli olarak saklanır ve bu ortamlara uygun yazılımlar kullanılarak silinmektedir.

### **7.1.4. Veri Tabanları**

Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (DELETE vb.) silinmesi gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilmelidir.

Şirket tarafından gerçekleştirilen tüm silme işlemleri elektronik ortamda zaman damgası ile loglanarak kayıt altına alınır. Kağıt ortamdaki kişisel veriler bakımından ise bu işlemlerin gerçekleştirildiğine ilişkin tutanak düzenlenir ve ilgili birim tarafından muhafaza edilir. Elektronik ve kağıt ortamdaki kişisel verilere ilişkin silmeye ilişkin kayıtlar üç yıl süre ile saklanır.

## **7.2. Kişisel Verilerin Yok Edilmesi**

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu olarak Şirketimiz yok edilen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli teknik ve idari tedbirleri almaktadır.

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi sağlanmaktadır.

### 7.2.1. Yerel Sistemler

Söz konusu sistemler üzerindeki verilerin yok edilmesi için;

- Fiziksel Yok Etme yöntemi kullanılarak; Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi sağlanmaktadır. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanmaktadır.
- Üzerine Yazma yöntemi kullanılarak; Manyetik medya ve yeniden yazılabilir optik medya üzerine en yaz yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmektedir. Bu işlem özel yazılımlar kullanılarak yapılmaktadır.

### 7.2.2. Çevresel Sistemler

Ortam türüne bağlı olarak kullanılacak yok etme yöntemleri;

- Ağ cihazları (switch, router vb.) içerisindeki sabit saklama ortamlarında yer alan veriler yukarıda belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmektedir.
- Flash tabanlı ortamların ATA (SATA, SSD, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları, destekleniyorsa <block erase> komutunu kullanmak, desteklenmiyorsa uygun diğer yöntemler kullanılmak suretiyle yok edilmektedir.
- Mobil telefonlar (Sim kart ve sabit hafıza alanları),
- Veri kayıt ortamı çıkartılabilir olan yazıcı gibi çevre birimleri,
- Veri kayıt ortamı sabit olan yazıcı, parmak izi kullanılan kapı geçiş sistemleri gibi çevre birimleri yukarıda erel sistemlerde belirtilen yöntemlerden uygun olanları kullanmak suretiyle yok edilmektedir.

### 7.2.3. Kağıt Ortamlar

Şirket yerleşkesinde kağıt ortamında saklanan kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazıldığı olduğundan ana ortamın kağıt imha veya kırpma makinaları ile anlaşılmaz

boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek suretiyle yok edilmektedir.

### **7.3. Kişisel Verilerin Anonim Hale Getirilmesi**

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir.

Anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyen bu işlemde sonra İlgili Kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

Şirketimiz, kişisel verilerin anonim haline getirilmesi için saklanmakta olan Kişisel Verilerin niteliğine ve risk-maliyet analizine göre uygun anonimleştirme yöntemlerinin belirlenmesini sağlayacaktır.

Veri sorumlusu sıfatıyla Şirketimiz, kişisel verilerin anonim hale getirilmesi için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür. Kişisel verilerin anonim hale getirilmesi, kişisel veri saklama ve imha politikasında belirtilen esaslara uygun olarak aşağıdaki yöntemlerle gerçekleştirilir.

#### **7.3.1. Değer Düzensizliği Sağlamayan Anonim Hale Getirme Yöntemleri**

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. Bu yöntemler aşağıdaki şekildedir;

##### **a) Değişken Çıkartma:**

Kişisel verileri oluşturan tanımlayıcılardan birinin veya birkaçının tablodan/sistemden bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir.

Burada dikkat edilmesi gereken, değişkenlerin çıkarılması halinde geriye kalan verilerden yola çıkarak ilgili gerçek kişinin eşleştirilemiyor olmasıdır. Örn; personel listesinin yer aldığı bir listede saklama sürelerinin dolmasının ardından yapılacak anonimleştirme uygulamasında, adrese ilişkin tanımlayıcı değişkenler kaldırılrsa da, kalan maaş bilgisinden yola çıkarak (söz

konusu maaş miktarına şirket içerisinde tek bir kişinin sahip olması gibi) ilgili kişiye erişimin sağlanması halinde bir başka değişkenin çıkarılması yolu kullanılacaktır.

**b) Kayıtları Çıkartma:**

Bu yöntemde saklanmakta olan kişisel veriler arasında bir değişkenin çıkarılmasındansa tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür.

Örneğin, burs listesinde herhangi bir üniversiteden/okuldan yalnızca tek bir kişinin yer alması durumunda tüm listeden okul adı değişkenini çıkartmaktansa, bu kişiye ait satırın tümü çıkartılacaktır.

**c) Bölgesel Gizleme:**

Bu yöntemin kullanılmasında asıl amaç, kişisel verinin sahip olduğu belirleyici özellik sebebiyle kişisel verilere erişimi bulunan kişiler tarafından tahmin edilebilirliğinin önüne geçebilmek amacıyla, belirleyici özellik taşıyan veri çıkarılarak diğer veriler yerinde tutulmak suretiyle anonimleştirme sağlanmış olacaktır.

Örneğin, şirketin etkinlik katılımcı listesinde yalnızca tek bir kişinin doğum yılı 1960'tan önce ise, medeni durum, katılım bilgisi, masa numarasının birlikte saklandığı bir veri kümesinde 'doğum yılı' sekmesinin boş bırakılması suretiyle ilgili kişinin eşleştirilebilirliğinin önüne geçilecektir.

**d) Genelleştirme**

Bu işlem, saklanmakta olan kişisel verinin tanımlayıcı nitelikte olan belirli bir değerden, eşleştirmeyi engelleyecek daha genel bir değere çevirme işlemidir. Örneğin; performans değerlendirme raporlarının toplu bir şekilde hazırlanması durumunda, departman bilgisinin kullanılması yerine çalışanların %...'sinin belirtilerek raporun hazırlanması gerçek bir kişiye erişmeyi imkansız hale getiren bir işlem olacaktır.

**e) Alt ve Üst Sınır Kodlama:**

Bu yöntem, belli bir değişken için bir kategori belirlenerek bu kategorinin içerisinde kalan değerlerin birleştirilmesi suretiyle kişisel verilerin anonim hale getirilmesi sağlanmaktadır.

Örneğin; Personel listesinde yer alan kıdem ve maaşa ilişkin değişkenler belli kategorilerde gruplandırılarak (ör; 24bin TL yıllık gelirden az olanlar düşük, 5 yıldan az kıdemi olanlar junior şeklinde gruplandırılarak, ücret ve kıdem sütununun altına yeni oluşturulan değerler girilmektedir)

#### **f) Global Kodlama:**

Bu yöntem rakamsal olarak gruplama yapılabilen alt ve üst sınır kodlamanın uygulanmasının mümkün olmadığı hallerde kullanılan gruplama vasıtasıyla anonim hale getirme yöntemidir. Önemli olan, veriye erişim sağlayabilen kişiler tarafından belirli değerlerin kümelenerek tahmin yürütmeyi kolaylaştırdığı hallerde kullanılır. İstenen bir veri değeri için ortak ve yeni bir grup oluşturulması suretiyle, veri kümesindeki tüm kayıtlar yeni tanım ile değiştirilmektedir.

Örneğin; müşterinin ikametgah adresi yerine semt adının yazılması.

#### **g) Örnekleme**

Bu yöntemde, veri kümesinin tamamı yerine, kişisel verileri içeren kümede yer alan bir alt kategori açıklanır veya aktarılır. Bu yöntem ile, bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığının tahmin edilemeyeceği için veriler anonim hale getirilmiş olur.

Örneğin; İstanbul ilinde yaşayan kadınların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir veri kümesinin anonim hale getirilerek açıklanması ya da paylaşılması halinde İstanbul'da yaşadığı bilinen bir kadına dair tahmin yürütmek mümkün olabileceken, söz konusu listede, sadece nüfusa kayıtlı olduğu il İstanbul olan kadınların kayıtları bırakılarak, nüfus kaydı diğer illerde olan kadınlar listeden çıkarılırsa, veriye erişim sağlayan kişi, İstanbul'da yaşadığını bildiği bir kadının nüfus kaydının İstanbul'da olup olmadığını tahmin edemeyeceğinden kişisel veriler anonim hale getirilmiş olacaktır.

### **7.3.2. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri**

Değer düzensizliği sağlayan anonim hale getirme yöntemlerinde yukarıda belirtilenlerin aksine kişisel veri gruplarında bazı verilerin değiştirilmesi ile bozulma ortaya çıkmaktadır. Bu yöntemler kullanılırken elde edilmek istenen yarara uyumlu olacak şekilde değişkenliklerin dikkatle uygulanması gerekmektedir. Ayrıca, verilerin güncel tutulmasının KVK Kanunu

kapsamında Veri Sorumlusuna yüklenmiş olan bir kural olduğu düşünülürken, değer düzensizliği sağlanması halinde ilgili kişinin verilerinin gerçeğe aykırı bir hale geldiği durumlarda söz konusu yöntemler uygulanmamalıdır.

**a) Mikro Birleştirme:**

Bu yöntem ile kişisel veri içeren veri kümesindeki bütün kayıtlar ilk olarak anlamlı bir sıraya göre dizilerek, sonrasında bütün kümenin belirli bir sayıda alt kümelere ayrılması sağlanır. Sonrasında, her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Bu şekilde, değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.

Örneğin; Kıdem süresi 5 yıldan az, 5- 10 yıl arası ve 15 yıldan fazla olan kişiler tespit edilerek, kıdem yılları kişi sayısına bölünmek suretiyle, kıdem süresinin ortalaması alınır, sonrasında kıdem yılı yerine her bir kıdem aralığında bulunan kişi için, o kıdem aralığında çıkan ortalama değer yazılmak suretiyle anonimleştirme sağlanmış olur.

**b) Veri Değiş Tokuşu:**

Bu yöntem, kişisel veri içeren kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeyle ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve asıl amaç değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesi suretiyle anonim hale getirme sürecinin sağlanmasıdır.

**c) Gürültü Ekleme:**

Bu yöntem, genel olarak sayısal verilerin bulunduğu bir veri kümesinde uygulanmakta olup, mevcut verilere belirlenen oranda artı veya eksi yönde birtakım sapmalar eşit ölçüde eklenerek veriler anonim hale getirilmektedir.

Örneğin, maaş bilgilerinin yer aldığı listede tüm personelin maaşına ayrı ayrı eşit ölçüde değer eklenip/çıkarılarak anonim hale getirme sağlanmış olur.

**d) İstatistiksel Yöntemler:**

Anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonim hale getirme süreci

güçlendirilmektedir. Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirmek suretiyle, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

### 7.3.3. Anonimlik Güvencesi

Şirketimiz tarafından, saklanmakta olan kişisel verilerin saklama sürelerinin dolmasının ardından silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmesi için aşağıdaki şartların sağlanmış olduğunun kontrolü gerçekleştirilmektedir;

- Anonim hale getirilmiş bir veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulmaması,
- Bir ya da birden fazla değer bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturamaması,
- Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

Şirketimiz yukarıda sayılan ihtimallerin ortadan kaldırılması amacıyla, Şirketimiz tarafından anonim hale getirilen veri kümeleri üzerinde bu maddede sayılan özellikler değişikçe kontroller gerçekleştirerek, anonimliğin korunduğundan emin olmak için gerekli tedbirleri yerine getirmeye çalışmaktadır.

## 8. KİŞİSEL VERİ SAKLAMA VE İMHA SÜREÇLERİNDE GÖREV VE SORUMLULUK DAĞILIMLARI

KVK Kanunu kapsamında Veri Sorumlularının yerine getirmesi gereken birçok yükümlülük bulunması ve Kişisel Verilerin İşlenmesi ve Hukuka Uygun Olarak Korunması yaşayan ve sürekli takip edilmesi gereken bir süreç olduğundan dolayı Veri Sorumlusu olarak Şirketimiz gerekli tedbirleri almaktadır.

Bu doğrultuda, B-PLAS Bursa Plastik Metal İnşaat Enerji Madencilik Jeotermal Turizm Sivil Havacılık ve Tarım Sanayi ve Ticaret Anonim Şirketi, kişisel verilerin işlenmesine, saklanması ve imhasına yönelik süreçlerin takibi, KVK Kanunu'na uyumluluğun sağlanması ve faaliyetlerinin KVK Kanunu'na uygun olarak yerine getirilebilmesi için, Şirketin Yönetim Kurulu kararı ile bünyesinde bir Kişisel Veri Koruma Komitesi ("KVK Komitesi") oluşturmuştur.

KVK Komitesi'nin başlıca görevleri:

- Mevzuat uyarınca yükümlülüklerini yerine getiren veri sorumlusuna, veri işleyene ve çalışanlarına bilgi vermek ve tavsiyede bulunmak,

- Veri sorumlusunun kişisel verilerin korunması ile ilgili politikalarının yanı sıra kişisel veri işlemede yer alan çalışanların bilinçlendirilmesi ve eğitilmesi ve ilgili denetimlerin mevzuata uygunluğunu takip etmek,
- Kişisel Verilerin İşlenmesi ve Kişisel Verilerin Saklanması ve İmhası Politikalarında yer alan kişisel veri işleme, saklama ve imhaya ilişkin teknik ve idari tedbirlerin uygulanmasının sağlanması,
- Kendisine yüklenen görevlerini yaparken, görevlerin yerine getirilebilmesi için gerekli parasal ve fiziksel kaynakları belirlemek, kişisel verilere ve işlemlere erişebilmesini sürdürebilmek,
- Belirlenen temel politika ve aksiyon adımlarını üst yönetimin onayına sunmak, uygulamasını gözetmek ve koordinasyonunu sağlamak,
- Kişisel veri sahiplerinin başvurularını hızlı bir şekilde karşılayacak bir mekanizma oluşturmak ve başvuruları en üst düzeyde karara bağlamak,
- Kişisel verilerin korunması konusundaki gelişmeleri takip etmek ve bu gelişmeler kapsamında yapılması gerekenler konusunda üst yönetime tavsiyelerde bulunmak,
- İlgili kişilerin verilerinin hukuka, Kişisel Verilerin İşlenmesi ve Korunması Politikasına ve Kişisel Verilerin Saklanması ve İmhası Politikasına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemek,
- Şirket, Yönetim Kurulu'un kişisel verilerin korunması ile ilgili süreçlere yönelik olarak vereceği talimatları ve görevleri yerine getirmek ile yetkili ve görevlidir.

Bununla birlikte B-PLAS Bursa Plastik Metal İnşaat Enerji Madencilik Jeotermal Turizm Sivil Havacılık ve Tarım Sanayi ve Ticaret Anonim Şirketi bünyesinde kişisel veri işleyen tüm departmanların sorumluları/yöneticileri, gerek kendi departmanlarının kişisel veri işleme envanterinin güncelliğinin sağlanması gerek kişisel veri saklama ve imha süreçlerinin takibi için bölümünde çalışan bir başka kişiyi görevlendirebilecektir.

KVK Komitesinin üyeleri, İK ve IT departmanından bir senior bir junior olmak üzere ikişer kişi, toplamda 4 kişilik personelden oluşmaktadır.

B-PLAS Bursa Plastik Metal İnşaat Enerji Madencilik Jeotermal Turizm Sivil Havacılık ve Tarım Sanayi ve Ticaret Anonim Şirketi KVK Komitesinde yer alan çalışanların unvan, birim ve görevlerine ilişkin bilgiler aşağıdaki tabloda yer almaktadır.



UNVAN	DEPARTMAN	GÖREV
İnsan Kaynakları Müdürü (İrtibat Kişisi)	<u>İnsan Kaynakları Departmanı</u> Kişisel verilerin işlenmesi, korunması, saklanması ve imhası uygulama sorumlusu	Kişisel Verilerin işlenmesine, korunmasına ve saklanmasına ilişkin süreçlerin işlerliğinin denetlenmesi, departman faaliyeti dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ve görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
İnsan Kaynakları Uzmanı	<u>İnsan Kaynakları Departmanı</u> Kişisel verilerin işlenmesi, korunması, saklanması ve imhası uygulama sorumlusu	Kişisel Verilerin işlenmesine, korunmasına ve saklanmasına ilişkin süreçlerin işlerliğinin denetlenmesi, departman faaliyeti dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanmasının yönetimi ve görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Bilgi İşlem Müdürü	<u>Bilgi Teknolojileri Departmanı</u> Kişisel verilerin işlenmesi, korunması, saklanması ve imhası uygulama sorumlusu	Kişisel Verilerin işlenmesine, korunmasına ve saklanmasına ilişkin süreçlerin işlerliğinin denetlenmesi, departman faaliyeti dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanmasının yönetimi ve görevi dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
Bilgi İşlem Uzmanı	<u>Bilgi Teknolojileri Departmanı</u> Kişisel verilerin işlenmesi, korunması, saklanması ve imhası uygulama sorumlusu	Kişisel Verilerin işlenmesine, korunmasına ve saklanmasına ilişkin süreçlerin işlerliğinin denetlenmesi, departman faaliyeti dahilinde olan süreçlerin saklama süresine uygunluğunun sağlanmasının yönetimi ve görevi dahilinde olan

		süreçlerin saklama süresine uygunluğunun sağlanması ile periyodik imha süresi uyarınca kişisel veri imha sürecinin yönetimi
--	--	---

## 9. SAKLAMA VE İMHA SÜRELERİ TABLOSU

Saklama ve imha süreleri tablosuna her bir departman bazında hazırlanmış Kişisel Veri İşleme Envanteri'nde yer verilmekte olup, işbu envanterde süreç bazında belirtilen süreler ile ilgili özet tablo aşağıda yer almaktadır. Bununla birlikte, kişisel veri kategori bazında belirlenmiş olan saklama süreleri Şirketimizin VERBİS kaydı esnasında bildirilmiştir.

Bu kapsamda işlenen kişisel veriler, aksine bir kesinleşmiş mahkeme kararı veya ihtiyati tedbir kararı bulunmadıkça işbu Saklama ve İmha Politika'sında belirtilen hususlar dikkate alınarak aşağıdaki tabloda belirtilen süreler boyunca saklanacak, süre sonunda ise imha edilecektir.

Kişisel Verileri Saklama ve İmha Süreleri'ni gösteren tablo kişisel veri işleme envanterinde yer alan süreçlerin yürütülmesinden sorumlu departmanlarca, tereddüt halinde KVK Komitesi değerlendirmeleri de alınarak güncellenebilecektir.

Şirket tarafından yürütülen iş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar doğmasına neden olacak periyodik imhalar, ilgili kişisel verinin kategorisi, kişisel verilerin yer aldığı ortamların özelliği ve ilgili kullanıcı tarafından dikkate alınarak ilgili uzman tarafından yapılacaktır.

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
İş Kanunu kapsamında saklanan veriler (örn; Kıdem tazminatı, İhbar tazminatı, Kötüniyet tazminatı, Eşit Davranma İlkesine aykırılık tazminatına konu olabilecek bilgiler; bordro kayıtları, yıllık izin gün sayısı vs.)	İş ilişkisinin sona ermesinden itibaren 5 yıl	4857 Sayılı İş Kanunu ve ilgili mevzuat	Saklama süresinin bitimini takiben 6 ay içerisinde

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
İş Kanunu kapsamında saklanan özlük dosyasına ilişkim veriler (örn; Kıdem tazminatı, İhbar tazminatı, Kötüniyet tazminatı, Eşit Davranma İlkesine aykırılık tazminatı dışındaki taleplere konu olabilecek bilgiler; bordro kayıtları, yıllık izin gün sayısı vs.)	İş ilişkisinin sona erdiği tarihten itibaren 10 yıl	4857 Sayılı İş Kanunu ve ilgili mevzuat/6098 sayılı Türk Borçlar Kanunu	Saklama süresinin bitimini takiben 6 ay içerisinde
İş Kanunu kapsamında saklanan verilerden Sendikal tazminata konu olabilecek veriler (örn; performans kayıtları, disiplin cezaları, fesih evrakları vs.)	İş ilişkisinin sona ermesinden itibaren 10 yıl	6098 sayılı Türk Borçlar Kanunu	Saklama süresinin bitimini takiben 6 ay içerisinde
İş sağlığı ve güvenliği mevzuatı kapsamında toplanan veriler (ör; işe giriş sağlık testleri, sağlık raporları, isg eğitimleri, iş sağlığı ve güvenliği faaliyetlerine ilişkin kayıtlar vs.)	İş ilişkisinin sona ermesinden itibaren 15 yıl	6331 sayılı İş Sağlığı ve Güvenliği Kanunu, İş Sağlığı ve Güvenliği Hizmetleri Yönetmeliği	Saklama süresinin bitimini takiben 6 ay içerisinde
SGK mevzuatı kapsamında tutulan veriler (örn; işe giriş bildireleri, prim/hizmet belgeleri)	İş ilişkisinin sona ermesine müteakip 10 yıl	5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu ve ilgili mevzuat	Saklama süresinin bitimini takiben 6 ay içerisinde
İş Kanunu uyarınca; çalışan ile ilgili mahkeme/icra bilgi taleplerinin cevaplanması	İş ilişkisinin sona ermesine müteakip 10 yıl	4357 Sayılı İş Kanunu ve ilgili mevzuat	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışan Erişim Kısıtlamaları-Active Directory işlemleri	İş ilişkisinin sona ermesine müteakip 10 yıl	4357 Sayılı İş Kanunu ve ilgili mevzuat	Saklama süresinin bitimini

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
			takiben 180 gün içerisinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler (ör: huzur hakkı ödemesi, kar payı)	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirket ortakları ve yönetim kurulu üyelerine ait bilgiler (pay defterinde yer alan kişisel veriler)	Pay defterinin saklanma zorunluluğu sebebiyle Süresiz	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Burs Ödemesi/Çalışan Avans Ödemesi	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
İş Başvurusu/staj Başvurusu/ Burs Başvurusunun kabul edilmediği takdirde Aday Başvurularına ilişkin veriler (ör; CV, Cover Letter, Başvuru formu vs.)	6 ay	Sektörel Teamül	Saklama süresinin bitimini takiben 180 gün içerisinde
Sendikal faaliyetler uyarınca işlenen ve sendika ile paylaşılan kişisel veriler	10 yıl	6356 Sayılı Sendikalar ve Toplu İş Sözleşmesi Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışanlara Yönelik Kurumsal İletişim Faaliyetleri uyarınca işlenen veriler (Ör; Katılımcı Listesi)	İş ilişkisinin sona ermesine müteakip 10 yıl	Sektörel Teamül	Saklama süresinin bitimini takiben 180 gün içerisinde

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
Çalışan Memnuniyet Anketlerine İlişkin Veriler	Anketin doldurulduğu yılın sona ermesine müteakip 1 yıl	Sektörel Teamül	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirket faaliyetleri uyarınca, saklanması gereken ticari defterler, ticari defterlerde yer alan kayıtlara dayanak oluşturan belgeler, finansal tablolar, vs uyarınca işlenebilecek kişisel veriler	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Genel Kurul İşlemleri uyarınca işlenen veriler	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Şirketin taraf olduğu sözleşmelerin kurulması ve içeriğine ilişkin kişisel veriler	10 yıl	6102 sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Mal ve hizmetleri tanıtmak, pazarlamak, işletmesini tanıtmak ya da kutlama ve temenni gibi içeriklerle tanınırlığı artırmak amacıyla alıcıların elektronik iletişim adreslerine gönderilen ticari elektronik iletilere ilişkin onay kayıtları	1 yıl	29417 sayılı 15.07.2015 tarihli Resmi Gazete’de yayımlanan Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmelik	Saklama süresinin bitimini takiben 180 gün içerisinde
Mal ve hizmetleri tanıtmak, pazarlamak, işletmesini tanıtmak ya da kutlama ve temenni gibi içeriklerle tanınırlığı artırmak amacıyla	1 yıl	29417 sayılı 15.07.2015 tarihli Resmi Gazete’de yayımlanan Ticari İletişim ve Ticari	Saklama süresinin bitimini takiben 180 gün içerisinde

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
alıcıların elektronik iletişim adreslerine gönderilen ticari elektronik iletilere ilişkin onay kayıtları dışındaki veriler		Elektronik İletiler Hakkında Yönetmelik	
Sözleşmeden kaynaklı ilişkilerde işlenen kişisel veriler (ör; şirket yetkilisi ad-soyad, imza sirküleri vs.)	Sözleşmenin sona ermesine müteakip 10 yıl	6098 sayılı Türk Borçlar Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Vergisel kayıtlara ilişkin kişisel veriler	5 Yıl	213 sayılı Vergi Usul Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Fatura/Gider pusulası/Makbuz gibi Vergi Usul Kanunu uyarınca tutulması gereken belgelerle işlenen kişisel veriler	5 yıl	213 Sayılı Vergi Usul Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Ziyaretçilerin kişisel verileri	2 yıl	5651 sayılı Kanun (Şirket wi-fi ağına erişim sağlayan ziyaretçiler açısından)	Saklama süresinin bitimini takiben 180 gün içerisinde
CCTV kameraları uyarınca güvenlik amaçlı olarak işlenen kişisel veriler (kamera kayıtları)	15 gün	Sektörel Teamül	Saklama süresinin bitimini takiben 180 gün içerisinde
Çalışanların Kişisel Verilerin yer aldığı ortamlara ilişkin yaptığı erişimlerin Log kayıtları	En az 2 yıl olmak suretiyle İş davalarına konu olabilmesi sebebiyle 10 yıl	5651 sayılı Kanun gereği ve TİB (Telekomünikasyon İletişim Başkanlığı) yönetmelikleri	Saklama süresinin bitimini takiben 180 gün içerisinde

Süreç	Saklama Süresi	Kanuni Dayanak	İmha Süresi
Şirket internet ağının kullanılması, İnternet Giriş ve Uzaktan Bağlantı esnasında işlenen Trafik bilgileri (ör;IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri vs)	2 yıl	5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşteri Bilgilerinden, TTK md.82 uyarınca ticari defter ve kayıtlara dayanak teşkil eden faturaların düzenlenmesine ilişkin kişisel veriler	10 yıl	6102 Sayılı Türk Ticaret Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Müşteri İşlem Bilgileri(Müşterilerin Talep/Şikayet/Önerilerine ilişkin Çağrı kayıtları vs.)	10 yıl	6098 sayılı Türk Borçlar Kanunu	Saklama süresinin bitimini takiben 180 gün içerisinde
Potansiyel Müşterilere ilişkin veriler (ör: cookies, linkedin üzerinden profillemeye ilişkin veriler)	13 ay	Avrupa Birliği/Sektörel Teamül uygulaması	Saklama süresinin bitimini takiben 180 gün içerisinde

## 10. PERİYODİK İMHA SÜRESİ

Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 11. maddesinde “*Kişisel veri saklama ve imha politikası hazırlamış olan 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.*” denmektedir.

Bu kapsamda Veri Sorumlusu olarak B-PLAS Bursa Plastik Metal İnşaat Enerji Madencilik Jeotermal Turizm Sivil Havacılık ve Tarım Sanayi ve Ticaret Anonim Şirketi saklama süresi sona

eren ve kişisel verinin saklanmasını gerektirecek başka herhangi bir veri işleme amacı mevcut olmayan kişisel verileri, saklama süresinin sona ermesini takiben 180 gün (6 ay) içerisinde anonim hale getirmektedir.

### **11. İLGİLİ KİŞİNİN TALEBİ ÜZERİNE SİLME VE YOK ETME SÜRELERİ**

İlgili kişi, B-PLAS Bursa Plastik Metal İnşaat Enerji Madencilik Jeotermal Turizm Sivil Havacılık ve Tarım Sanayi ve Ticaret Anonim Şirketi'ne başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde, Şirketimiz;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; talebe konu kişisel verileri işbu politika uyarınca siler, yok eder veya anonim hale getirir. Şirket, ilgili kişilerin silme veya yok etme taleplerini en geç **“otuz gün”** içinde sonuçlandırır.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa; bu durumu aktarım yapılan üçüncü kişiye bildirerek söz konusu kişisel verilerin silinmesi veya yok edilmesini talep eder.

Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Kişisel Verilerin Korunması Kanunu'nun 13. maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç **“otuz gün”** içinde, ilgili kişinin talebine uygun olarak, yazılı olarak ya da elektronik ortamda bildirilir.

### **12. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI POLİTİKASINDA YAPILACAK GÜNCELLEMELER**

Şirket, KVK Kanunu'nda yapılan değişiklikler nedeniyle, KVK Kurumu kararları uyarınca ya da ortaya çıkacak gelişmeler doğrultusunda, Kişisel Verilerin İşlenmesi ve Korunması Politikasında ya da işbu Kişisel Verilerin Saklanması ve İmhası Politikasında değişiklik yapma hakkını saklı tutmaktadır.

İşbu Kişisel Verilerin Saklanması ve İmhası Politikasında yapılan değişiklikler derhal metne işlenir ve değişikliklere ilişkin açıklamalar politikanın sonunda açıklanır. İşbu politikada yapılacak güncellemeler Şirket tarafından onaylanması üzerine revizyon ve onay tarihi ile birlikte <https://www.bplas.com.tr> adresinde, kurumsal intranet ağı içerisinde yayımlar.



**13. YÜRÜRLÜK**

İşbu Kişisel Verilerin Saklanması ve İşlenmesi Politikası ve ileride yapılacak güncellemeler, <https://www.bplas.com.tr> adresinde yayımlanacak olup, ayrıca, Şirketimizin kurumsal intranet ağı üzerinden çalışanlarımızın erişimine sunulacaktır.

<b>DÖKÜMAN GÜNCELLEME TABLOSU</b>				
<b>Politika Maddesi</b>	<b>Politika Alt Maddesi</b>	<b>Versiyon</b>	<b>Yayın Tarihi</b>	<b>Değişikliğin Tanımı</b>
		1.1	.....2021	Kişisel Verilerin Saklanmasına ve İmhasına İlişkin Politika