KİŞİSEL VERİLERİN KORUNMASI VE İŞLENMESİ POLİTİKASI

1. AMAÇ

Lider Faktoring A.Ş. ("Şirket") kişisel verilerin korunmasını, bireylerin temel hak ve özgürlüklerinin korunmasının ayrılmaz bir parçası olarak kabul etmektedir. İşbu Kişisel Verilerin Korunması ve İşlenmesi Politikası ("Politika"), Şirket tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinin 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK"), ilgili ikincil düzenlemeler, Kişisel Verileri Koruma Kurulu kararları ve diğer ilgili mevzuata uygun şekilde yürütülmesine ilişkin temel esas ve prensipleri belirlemek amacıyla hazırlanmıştır.

Bu Politika ile;

• Şirket tarafından işlenen kişisel verilerin hukuka uygun şekilde işlenmesinin sağlanması,
• Kişisel verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması,
• Veri güvenliği kültürünün kurum genelinde yaygınlaştırılması,
• İlgili kişilerin hak ve özgürlüklerinin korunması,
• Şirket bünyesinde gerçekleştirilen kişisel veri işleme faaliyetlerinde standart uygulamaların oluşturulması,
• Kişisel veri işleme faaliyetlerine ilişkin kurumsal yönetişim yapısının belirlenmesi,
• Veri güvenliği risklerinin etkin şekilde yönetilmesi,

amaçlanmaktadır.

Şirket, kişisel verilerin işlenmesinde hukuka uygunluk, dürüstlük, şeffaflık, hesap verebilirlik ve veri minimizasyonu ilkelerini esas almakta olup, kişisel verilerin korunmasını kurumsal risk yönetiminin önemli bir unsuru olarak değerlendirmektedir.

2. KAPSAM

Bu Politika;

• Şirket müşterilerini,
• Potansiyel müşterileri,
• Borçluları,
• Kefilleri,
• Çalışanları,
• Çalışan adaylarını,
• Stajyerleri,
• Eski çalışanları,
• Hissedarları,
• Yönetim kurulu üyelerini,
• Tedarikçileri,
• Hizmet sağlayıcıları,
• İş ortaklarını,
• Ziyaretçileri,
• Şirket ile herhangi bir hukuki veya ticari ilişki içerisinde bulunan diğer gerçek kişileri,

kapsamaktadır.

Politika, kişisel verilerin tamamen veya kısmen otomatik yollarla işlenmesi ile herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenmesine uygulanır.

Şirket bünyesinde yürütülen tüm faaliyetler kapsamında elde edilen, kaydedilen, depolanan, muhafaza edilen, aktarılan, açıklanan, sınıflandırılan veya üzerinde herhangi bir işlem gerçekleştirilen kişisel veriler işbu Politika kapsamında değerlendirilir.

3. DAYANAK

Bu Politika aşağıdaki mevzuat ve düzenlemeler esas alınarak hazırlanmıştır:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- 6361 sayılı Finansal Kiralama, Faktoring, Finansman ve Tasarruf Finansman Şirketleri Kanunu,
- 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun,
- 4857 sayılı İş Kanunu,
- 6098 sayılı Türk Borçlar Kanunu,
- 5237 sayılı Türk Ceza Kanunu,
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik,
- Veri Sorumluları Sicili Hakkında Yönetmelik,
- Kişisel Verileri Koruma Kurulu kararları,
- Bankacılık Düzenleme ve Denetleme Kurumu düzenlemeleri,
- Mali Suçları Araştırma Kurulu düzenlemeleri,
- Diğer ilgili mevzuat hükümleri.

İlgili mevzuatta değişiklik olması halinde Politika hükümleri gözden geçirilir ve gerekli güncellemeler yapılır.

4. TANIMLAR

Bu Politikada yer alan kavramlar aşağıdaki anlamları ifade eder:

Açık Rıza: Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızayı,
Anonim Hale Getirme: Kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,
İlgili Kişi: Kişisel verisi işlenen gerçek kişiyi,
Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,
Özel Nitelikli Kişisel Veri: KVKK kapsamında özel koruma gerektiren kişisel verileri,
Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel veri işleyen gerçek veya tüzel kişiyi,
Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,
Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen Lider Faktoring A.Ş.'yi,
KVKK: 6698 sayılı Kişisel Verilerin Korunması Kanunu'nu,
Kurul: Kişisel Verileri Koruma Kurulu'nu,
Kurum: Kişisel Verileri Koruma Kurumu'nu,

ifade eder.

5. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN TEMEL İLKELER

Şirket tarafından gerçekleştirilen tüm kişisel veri işleme faaliyetlerinde aşağıdaki temel ilkeler esas alınır.

5.1 Hukuka ve Dürüstlük Kurallarına Uygun Olma

Kişisel veriler hukuka uygun, dürüstlük kurallarına bağlı ve ilgili kişilerin temel hak ve özgürlüklerine saygılı şekilde işlenir.

5.2 Doğru ve Gerektiğinde Güncel Olma

Şirket, kişisel verilerin doğru ve güncel tutulması için gerekli makul tedbirleri alır. Güncellenmesi gereken verilerin düzeltilmesine yönelik süreçler oluşturulur.

5.3 Belirli, Açık ve Meşru Amaçlarla İşlenme

Kişisel veriler yalnızca belirlenmiş, açıkça tanımlanmış ve hukuka uygun amaçlar doğrultusunda işlenir.

5.4 İşlendikleri Amaçla Bağlantılı, Sınırlı ve Ölçülü Olma

Kişisel veri işleme faaliyetlerinde veri minimizasyonu ilkesi esas alınır. İşleme amacıyla ilgisiz veya gereksiz veri işlenmez.

5.5 İlgili Mevzuatta Öngörülen veya İşlendikleri Amaç İçin Gerekli Süre Kadar Muhafaza Edilme

Kişisel veriler yalnızca ilgili mevzuatın öngördüğü süre boyunca veya işleme amacının gerektirdiği süre kadar saklanır. Sürenin sona ermesi halinde veriler silinir, yok edilir veya anonim hale getirilir.

6. KURUMSAL YÖNETİM VE KVKK YÖNETİŞİM MODELİ

Şirket, kişisel verilerin korunmasını yalnızca hukuki bir yükümlülük olarak değil, aynı zamanda kurumsal yönetişim anlayışının temel unsurlarından biri olarak değerlendirmektedir.

Kişisel verilerin korunmasına ilişkin faaliyetlerin etkin şekilde yönetilebilmesi amacıyla görev, yetki ve sorumluluklar aşağıdaki şekilde belirlenmiştir.

6.1 Yönetim Kurulu

Yönetim Kurulu;

- KVKK uyum programının gözetiminden,
- Bu Politikanın onaylanmasından,
- Kişisel veri koruma kültürünün geliştirilmesinden,
- Veri güvenliği risklerinin üst düzeyde değerlendirilmesinden,

sorumludur.

6.2 Genel Müdürlük

Genel Müdürlük;

• Politikanın uygulanmasını sağlar,
• Gerekli kaynakları tahsis eder,
• Uyum faaliyetlerini koordine eder,
• Birimler arası koordinasyonu sağlar.

6.3 İnsan Kaynakları Müdürlüğü

İnsan Kaynakları Müdürlüğü;

• Çalışan verilerinin işlenmesi,
• Aydınlatma süreçlerinin yürütülmesi,
• Çalışan taahhütnamelerinin yönetimi,
• KVKK eğitimlerinin organizasyonu,

konularından sorumludur.

6.4 Bilgi Teknolojileri Birimi

Bilgi Teknolojileri Birimi;

• Teknik güvenlik tedbirlerinin uygulanması,
• Ağ ve sistem güvenliğinin sağlanması,
• Erişim yönetimi,
• Log yönetimi ve siber güvenlik faaliyetlerinin yürütülmesi,

konularından sorumludur.

6.5 İç Kontrol ve İç Denetim Birimleri

İç Kontrol ve İç Denetim Birimleri;

• KVKK uyum faaliyetlerini izler,
• Politikanın uygulanmasını denetler,
• Bulguları üst yönetime raporlar,
• Düzeltici faaliyetlerin takibini gerçekleştirir.

6.6 Çalışanlar

Şirket çalışanları;

• Kişisel verilerin korunmasına ilişkin politika ve prosedürlere uymak,
• Görevleri kapsamında eriştikleri kişisel verilerin gizliliğini korumak,
• Veri güvenliği ihlallerini gecikmeksizin bildirmek,

yükümlülüğü altındadır.

7. KİŞİSEL VERİ KATEGORİLERİ

Şirket faaliyetlerinin niteliği, yasal yükümlülükleri ve iş süreçleri kapsamında aşağıdaki kişisel veri kategorileri işlenebilmektedir.

7.1 Kimlik Bilgileri

Ad, soyad, T.C. kimlik numarası, doğum tarihi ve yeri, anne ve baba adı, nüfus cüzdanı bilgileri, imza bilgileri ve kimlik tespitine yarayan diğer bilgiler.

7.2 İletişim Bilgileri

Adres bilgileri, telefon numaraları, elektronik posta adresleri, kayıtlı elektronik posta (KEP) adresleri ve diğer iletişim bilgileri.

7.3 Müşteri İşlem Bilgileri

Faktoring işlemlerine ilişkin bilgiler, müşteri numarası, işlem kayıtları, sözleşme bilgileri, tahsilat bilgileri, borç ve alacak bilgileri ile müşteri ilişkileri kapsamında oluşan kayıtlar.

7.4 Finansal Bilgiler

Banka hesap bilgileri, ödeme bilgileri, gelir bilgileri, mali durum bilgileri, kredi ve risk değerlendirme verileri, finansal yükümlülüklere ilişkin bilgiler.

7.5 Hukuki İşlem Bilgileri

Dava ve icra dosyalarına ilişkin bilgiler, ihtarnameler, resmi kurum yazışmaları, vekâlet bilgileri ve hukuki süreçlere ilişkin kayıtlar.

7.6 İnsan Kaynakları ve Özlük Bilgileri

İşe giriş ve çıkış bilgileri, özlük dosyası kayıtları, bordro bilgileri, izin kayıtları, performans değerlendirmeleri, disiplin süreçleri ve kariyer gelişimine ilişkin bilgiler.

7.7 Eğitim ve Mesleki Deneyim Bilgileri

Diploma bilgileri, sertifikalar, mesleki yeterlilik belgeleri, özgeçmiş bilgileri ve eğitim kayıtları.

7.8 İşlem Güvenliği Bilgileri

IP kayıtları, sistem erişim kayıtları, log kayıtları, kullanıcı hesap bilgileri, parola yönetimi kayıtları ve elektronik işlem güvenliğine ilişkin diğer bilgiler.

7.9 Fiziksel Mekân Güvenliği Bilgileri

Kamera kayıtları, ziyaretçi giriş çıkış kayıtları, kartlı geçiş kayıtları ve bina güvenliğine ilişkin bilgiler.

7.10 Görsel ve İşitsel Veriler

Fotoğraflar, ses kayıtları, görüntülü görüşme kayıtları ve benzeri veriler.

7.11 Özel Nitelikli Kişisel Veriler

Sağlık verileri, adli sicil kayıtları ve ilgili mevzuat kapsamında işlenmesine izin verilen diğer özel nitelikli kişisel veriler.

8. KİŞİSEL VERİLERİN İŞLENME AMAÇLARI

Şirket tarafından kişisel veriler aşağıdaki amaçlarla işlenebilmektedir.

8.1 Faktoring Faaliyetlerinin Yürütülmesi

6361 sayılı Kanun kapsamında yürütülen faktoring faaliyetlerinin yerine getirilmesi, müşteri ilişkilerinin yönetilmesi ve sözleşmesel yükümlülüklerin yerine getirilmesi.

8.2 Müşteri Tanıma ve Risk Yönetimi Süreçleri

Kimlik doğrulama faaliyetlerinin yürütülmesi, müşteri tanıma yükümlülüklerinin yerine getirilmesi, kredi ve risk değerlendirme süreçlerinin yürütülmesi.

8.3 Yasal ve Düzenleyici Yükümlülüklerin Yerine Getirilmesi

BDDK, MASAK, TCMB ve diğer yetkili kurumlar tarafından öngörülen yükümlülüklerin yerine getirilmesi.

8.4 İnsan Kaynakları Süreçlerinin Yönetimi

İşe alım süreçlerinin yürütülmesi, personel özlük işlemleri, ücret yönetimi, performans değerlendirmeleri, eğitim faaliyetleri ve iş sözleşmelerinin yönetimi.

8.5 Bilgi Güvenliği Süreçlerinin Yönetimi

Bilgi sistemlerinin güvenliğinin sağlanması, yetkisiz erişimlerin önlenmesi ve siber güvenlik faaliyetlerinin yürütülmesi.

8.6 Hukuki Süreçlerin Takibi

Şirketin taraf olduğu dava, icra ve diğer hukuki süreçlerin yürütülmesi.

8.7 İç Kontrol ve İç Denetim Faaliyetleri

Kurumsal risk yönetimi, iç kontrol faaliyetleri ve iç denetim süreçlerinin yürütülmesi.

8.8 Finansal ve Operasyonel Raporlama

Yönetim raporlarının hazırlanması, bağımsız denetim faaliyetleri ve finansal raporlama süreçlerinin yürütülmesi.

8.9 İş Sürekliliği ve Operasyonel Güvenlik

Şirket faaliyetlerinin kesintisiz şekilde yürütülmesinin sağlanması ve operasyonel risklerin yönetilmesi.

9. KİŞİSEL VERİLERİN İŞLENME ŞARTLARI

Şirket tarafından kişisel veriler KVKK'nın 5. ve 6. maddelerinde belirtilen işleme şartlarına uygun olarak işlenmektedir.

Kişisel veriler aşağıdaki hukuki sebeplerden en az birinin varlığı halinde işlenebilir:

• Kanunlarda açıkça öngörülmesi,
• Bir sözleşmenin kurulması veya ifasıyla doğrudan ilgili olması,
• Şirketin hukuki yükümlülüğünü yerine getirmesi,
• Bir hakkın tesisi, kullanılması veya korunması için zorunlu olması,
• İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla Şirketin meşru menfaatleri için zorunlu olması,
• İlgili kişinin açık rızasının bulunması.

Şirket, kişisel verilerin işlenmesinde ilgili mevzuatın öngördüğü tüm yükümlülüklere uygun hareket eder.

10. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN İŞLENMESİ

Şirket tarafından işlenebilecek özel nitelikli kişisel veriler KVKK ve ilgili mevzuatta belirtilen şartlara uygun olarak işlenmektedir.

Özel nitelikli kişisel verilerin işlenmesinde;

• Erişim yetkilerinin sınırlandırılması,
• Yetki matrisi uygulanması,
• Şifreleme yöntemlerinin kullanılması,
• Log kayıtlarının tutulması,
• Gizlilik yükümlülüklerinin uygulanması,
• Güvenli saklama ortamlarının kullanılması,
• Düzenli denetim faaliyetlerinin gerçekleştirilmesi,

esas alınmaktadır.

Özel nitelikli kişisel verilere yalnızca görev tanımları gereği erişim yetkisine sahip kişiler erişebilir.

11. KİŞİSEL VERİLERİN AKTARILMASI

Şirket tarafından işlenen kişisel veriler, KVKK'nın 8. maddesine uygun olarak ve gerekli güvenlik önlemleri alınmak suretiyle aktarılabilmektedir.

Kişisel veriler aşağıdaki alıcı gruplarına aktarılabilir:

• Bankacılık Düzenleme ve Denetleme Kurumu (BDDK),
• Mali Suçları Araştırma Kurulu (MASAK),
• Türkiye Cumhuriyet Merkez Bankası (TCMB),
• Mahkemeler ve icra müdürlükleri,
• Yetkili kamu kurum ve kuruluşları,

• Bağımsız denetim kuruluşları,
• Hukuk büroları,
• Mali müşavirlik ve danışmanlık hizmeti alınan kuruluşlar,
• Bilgi teknolojileri hizmet sağlayıcıları,
• İş ortakları ve tedarikçiler,
• Kanunen yetkili diğer kişi ve kuruluşlar.

Kişisel veri aktarımlarında veri minimizasyonu ilkesi gözetilir ve yalnızca gerekli veriler paylaşılır.

12. KİŞİSEL VERİLERİN YURT DIŞINA AKTARILMASI

Şirket tarafından gerçekleştirilecek yurt dışı veri aktarımlarında KVKK'nın ilgili hükümleri esas alınır.

Yurt dışına veri aktarımı aşağıdaki hallerde gerçekleştirilebilir:

• Kişisel Verileri Koruma Kurulu tarafından ilgili ülke veya uluslararası kuruluş hakkında yeterlilik kararı verilmiş olması,
• Kanunda öngörülen uygun güvencelerin sağlanması,
• Standart sözleşmelerin kullanılması,
• Bağlayıcı şirket kurallarının uygulanması,
• KVKK'da belirtilen arızi aktarım şartlarının gerçekleşmesi.

Yurt dışına veri aktarımı yapılması halinde gerekli teknik ve idari güvenlik tedbirleri uygulanır ve ilgili mevzuat hükümlerine uyulur.

13. KİŞİSEL VERİLERİN GÜVENLİĞİ

13.1 Genel Esaslar

Lider Faktoring A.Ş., kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini, değiştirilmesini, açıklanmasını veya kaybedilmesini önlemek amacıyla KVKK'nın 12. maddesi kapsamında gerekli teknik ve idari tedbirleri almayı taahhüt eder.

Şirket, kişisel veri güvenliğini kurumsal risk yönetimi sisteminin ayrılmaz bir parçası olarak değerlendirmekte olup, bilgi güvenliği süreçlerini sürekli iyileştirme anlayışı ile yönetmektedir.

Kişisel verilerin korunmasına yönelik güvenlik tedbirleri belirlenirken;

• Veri kategorileri,
• Veri işleme faaliyetlerinin niteliği,
• Veri işleme amaçları,
• Veri güvenliği riskleri,
• Teknolojik gelişmeler,
• Yasal yükümlülükler,

dikkate alınmaktadır.

13.2 Veri Güvenliği Hedefleri

Şirket veri güvenliği faaliyetlerinde aşağıdaki hedefleri esas alır:

• Kişisel verilerin gizliliğinin korunması,
• Kişisel verilerin bütünlüğünün korunması,
• Kişisel verilerin erişilebilirliğinin sağlanması,
• Yetkisiz erişimlerin önlenmesi,
• Veri kayıplarının önlenmesi,
• Siber tehditlere karşı korunma sağlanması,
• Mevzuata uyumun sürdürülmesi.

13.3 Risk Temelli Yaklaşım

Şirket, kişisel veri güvenliğini risk temelli yaklaşımla yönetir.

Veri işleme faaliyetlerinden kaynaklanan riskler düzenli olarak değerlendirilir ve gerekli görülen teknik ve idari önlemler uygulanır.

14. TEKNİK VE İDARİ TEDBİRLER

14.1 Teknik Tedbirler

Şirket tarafından kişisel verilerin korunması amacıyla aşağıdaki teknik tedbirler uygulanabilir:

• Ağ güvenliği sistemleri,
• Güvenlik duvarları (Firewall),
• Antivirüs ve uç nokta koruma sistemleri,
• Erişim kontrol sistemleri,
• Kullanıcı yetkilendirme mekanizmaları,
• Çok faktörlü kimlik doğrulama sistemleri (MFA),
• Şifreleme yöntemleri,
• Log kayıtlarının tutulması ve izlenmesi,
• Düzenli veri yedekleme faaliyetleri,
• Veri kaybı önleme sistemleri (DLP),
• Güvenlik açıklarının izlenmesi,
• Sızma testleri ve zafiyet taramaları,
• Güvenli yazılım geliştirme uygulamaları,
• Ağ segmentasyonu uygulamaları,
• Felaket kurtarma sistemleri.

14.2 İdari Tedbirler

Şirket tarafından kişisel verilerin korunması amacıyla aşağıdaki idari tedbirler uygulanabilir:

• Politika ve prosedürlerin oluşturulması,
• Çalışan gizlilik taahhütnameleri,
• KVKK farkındalık eğitimleri,
• Bilgi güvenliği eğitimleri,
• Yetki matrisi uygulamaları,
• Görev ayrılığı prensiplerinin uygulanması,

• Risk analizleri,
• İç kontrol faaliyetleri,
• İç denetim faaliyetleri,
• Tedarikçi değerlendirme süreçleri,
• Gizlilik hükümleri içeren sözleşmeler,
• Düzenli mevzuat uyum kontrolleri.

14.3 Yetki Yönetimi

Kişisel verilere erişim, görev tanımları ve iş ihtiyaçları doğrultusunda sınırlandırılır.

Erişim yetkileri düzenli olarak gözden geçirilir.

Görev değişikliği veya iş ilişkisinin sona ermesi halinde ilgili erişim yetkileri gecikmeksizin kaldırılır.

15. KİŞİSEL VERİ İHLALİ YÖNETİMİ

15.1 Veri İhlali Tanımı

Kişisel verilerin;

• Yetkisiz kişiler tarafından ele geçirilmesi,
• Yetkisiz erişime maruz kalması,
• Hukuka aykırı şekilde paylaşılması,
• Kaybedilmesi,
• Değiştirilmesi,
• Yok edilmesi,

sonuçlarını doğuran veya doğurma ihtimali bulunan olaylar kişisel veri ihlali olarak değerlendirilir.

15.2 Veri İhlalinin Bildirilmesi

Şirket çalışanları ve hizmet sağlayıcıları kişisel veri ihlali şüphesi doğuran herhangi bir olayı gecikmeksizin yöneticilerine ve ilgili birimlere bildirmekle yükümlüdür.

Veri ihlali bildirimleri kayıt altına alınır ve değerlendirilir.

15.3 İhlal Yönetim Süreci

Veri ihlali meydana gelmesi halinde;

• Olayın kapsamı belirlenir,
• Etkilenen veri kategorileri tespit edilir,
• Etkilenen kişi grupları belirlenir,
• Risk analizi gerçekleştirilir,
• Teknik ve idari önlemler uygulanır,
• Gerekli bildirim süreçleri başlatılır,
• Düzeltici ve önleyici faaliyetler planlanır.

15.4 Yetkili Makamlara Bildirim

Kişisel veri ihlali meydana gelmesi halinde KVKK ve ilgili mevzuat kapsamında gerekli görülmesi durumunda Kişisel Verileri Koruma Kurulu'na ve ilgili kişilere bildirim yapılır.

15.5 İhlal Kayıtları

Tüm veri ihlalleri ve veri ihlali şüpheleri kayıt altına alınır.

Kayıtlar düzenli olarak analiz edilir ve tekrar eden risklere karşı iyileştirici faaliyetler yürütülür.

16. KİŞİSEL VERİLERİN SAKLANMASI VE İMHASI

16.1 Saklama İlkeleri

Şirket, kişisel verileri yalnızca ilgili mevzuatta öngörülen süre boyunca veya işleme amacının gerektirdiği süre kadar muhafaza eder.

Saklama sürelerinin belirlenmesinde;

• Kanuni yükümlülükler,
• Düzenleyici kurum gereklilikleri,
• Sözleşmesel yükümlülükler,
• Zamanaşımı süreleri,
• Şirketin meşru menfaatleri,

esas alınır.

16.2 İmha İlkeleri

İşleme amacının ortadan kalkması veya saklama süresinin sona ermesi halinde kişisel veriler;

• Silinir,
• Yok edilir,
• Anonim hale getirilir.

16.3 Periyodik İmha

Şirket tarafından hazırlanan Saklama ve İmha Politikası doğrultusunda periyodik imha faaliyetleri gerçekleştirilir.

Periyodik imha süreçleri kayıt altına alınır.

16.4 Güvenli İmha

Fiziksel ve elektronik ortamlarda bulunan kişisel verilerin imhası sırasında verilerin geri getirilemeyecek şekilde ortadan kaldırılması sağlanır.

17. VERİ ENVANTERİ VE VERBİS YÖNETİMİ

17.1 Veri İşleme Envanteri

Şirket, gerçekleştirdiği kişisel veri işleme faaliyetlerini Veri İşleme Envanteri kapsamında kayıt altına alır.

Envanterde;

• Veri kategorileri,
• İlgili kişi grupları,
• İşleme amaçları,
• Hukuki sebepler,
• Alıcı grupları,
• Saklama süreleri,
• Güvenlik tedbirleri,

yer alır.

17.2 Envanterin Güncellenmesi

Veri işleme faaliyetlerinde meydana gelen değişiklikler doğrultusunda Veri İşleme Envanteri güncellenir.

İlgili birimler envanter güncellemelerinde gerekli desteği sağlar.

17.3 VERBİS Yönetimi

Şirket, Veri Sorumluları Sicili Bilgi Sistemi (VERBİS) yükümlülüklerini ilgili mevzuata uygun şekilde yerine getirir.

VERBİS kayıtlarının güncelliği düzenli olarak kontrol edilir.

17.4 Periyodik Gözden Geçirme

Veri işleme faaliyetleri, veri kategorileri ve aktarım süreçleri yılda en az bir kez gözden geçirilir.

Gerekli görülmesi halinde güncelleme faaliyetleri gerçekleştirilir.

18. İLGİLİ KİŞİ HAKLARI VE BAŞVURU SÜRECİ

18.1 İlgili Kişi Hakları

KVKK'nın 11. maddesi uyarınca ilgili kişiler Şirkete başvurarak aşağıdaki haklarını kullanabilirler:

- Kişisel veri işlenip işlenmediğini öğrenme,
- Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,
- Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,
- Kişisel verilerin yurt içinde veya yurt dışında aktarıldığı üçüncü kişileri bilme,
- Eksik veya yanlış işlenmiş kişisel verilerin düzeltilmesini isteme,

- KVKK'nın 7. maddesi kapsamında kişisel verilerin silinmesini veya yok edilmesini isteme,
- Düzeltme, silme veya yok etme işlemlerinin aktarıldığı üçüncü kişilere bildirilmesini isteme,
- İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,
- Kişisel verilerin kanuna aykırı işlenmesi nedeniyle zarara uğraması halinde zararın giderilmesini talep etme.

18.2 Başvuru Yöntemleri

İlgili kişiler taleplerini;

- Yazılı başvuru,
- Noter aracılığıyla,
- KEP adresi üzerinden,
- Güvenli elektronik imza kullanarak,
- KVKK ve ilgili mevzuatta belirlenen diğer yöntemlerle

Şirkete iletebilirler.

18.3 Başvuruların Değerlendirilmesi

Başvurular ilgili mevzuatta belirtilen süreler içerisinde değerlendirilir.

Şirket gerekli gördüğü durumlarda başvuru sahibinden kimlik doğrulamasına yönelik ek bilgi ve belge talep edebilir.

19. EĞİTİM VE FARKINDALIK

19.1 Eğitim Politikası

Şirket, kişisel verilerin korunması kültürünün oluşturulması ve sürdürülmesi amacıyla çalışanlarına düzenli eğitimler verir.

19.2 Eğitim Kapsamı

Eğitimlerde aşağıdaki konulara yer verilebilir:

- KVKK temel prensipleri,
- Kişisel veri işleme şartları,
- Özel nitelikli kişisel veriler,
- Veri güvenliği yükümlülükleri,
- Bilgi güvenliği farkındalığı,
- Sosyal mühendislik saldırıları,
- Siber güvenlik tehditleri,
- Veri ihlali bildirim süreçleri,
- Çalışan sorumlulukları.

19.3 Eğitim Periyotları

KVKK eğitimleri;

- İşe girişlerde,
- Görev değişikliklerinde,
- Mevzuat değişikliklerinde,
- Yılda en az bir kez periyodik olarak

gerçekleştirilebilir.

20. DENETİM VE İZLEME

20.1 Denetim Faaliyetleri

Şirket, kişisel veri işleme faaliyetlerinin mevzuata uygunluğunu sağlamak amacıyla gerekli denetim faaliyetlerini gerçekleştirir.

20.2 İç Kontrol Faaliyetleri

İç Kontrol Birimi;

- KVKK süreçlerinin uygulanmasını,
- Veri güvenliği tedbirlerini,
- Politika ve prosedürlere uyumu

izler ve değerlendirir.

20.3 İç Denetim Faaliyetleri

İç Denetim Birimi risk esaslı yaklaşım çerçevesinde KVKK süreçlerine ilişkin denetimler gerçekleştirebilir.

20.4 Düzeltici Faaliyetler

Denetimlerde tespit edilen uygunsuzluklara ilişkin düzeltici ve önleyici faaliyetler planlanır ve takip edilir.

21. UYGUNSUZLUKLAR VE YAPTIRIMLAR

21.1 Genel Esas

Tüm çalışanlar işbu Politika hükümlerine uygun hareket etmekle yükümlüdür.

21.2 Çalışan Sorumluluğu

Çalışanlar;

- Görevleri nedeniyle eriştikleri kişisel verilerin gizliliğini korumak,
- Yetkisiz erişimleri önlemek,
- Şirket politika ve prosedürlerine uymak,

- Veri ihlallerini gecikmeksizin bildirmek

zorundadır.

21.3 Disiplin Süreçleri

Politika hükümlerine aykırı davranan çalışanlar hakkında;

- Disiplin prosedürleri,
- İş sözleşmesi hükümleri,
- İş Kanunu hükümleri,
- KVKK hükümleri,
- Türk Ceza Kanunu hükümleri

çerçevesinde işlem tesis edilebilir.

21.4 Tazminat ve Hukuki Sorumluluk

Mevzuata aykırı veri işleme faaliyetlerinden kaynaklanan hukuki ve cezai sorumluluk ilgili mevzuat hükümlerine göre değerlendirilir.

22. YÜRÜRLÜK VE REVİZYON

22.1 Yürürlük

Şirketimiz tarafından düzenlenen bu Politika 20.07.2026 tarihlidir.

Politika Şirketimizin internet sitesinde (www.liderfaktoring.com.tr) yayımlanır ve kişisel veri sahiplerinin talebi üzerine ilgili kişilerin erişimine sunulur.

22.2 Gözden Geçirme

Politika;

- Mevzuat değişikliklerinde,
- Organizasyonel değişikliklerde,
- Yeni risklerin ortaya çıkması halinde,
- En az yılda bir kez

gözden geçirilir.

22.3 Revizyon Yönetimi

Politikada yapılan değişiklikler revizyon tablosunda kayıt altına alınır.

EK-1 VERİ KATEGORİLERİ MATRİSİ

Veri Kategorisi	**İlgili Kişi Grubu**
Kimlik Bilgileri	Müşteri, Çalışan, Tedarikçi
İletişim Bilgileri	Müşteri, Çalışan, Tedarikçi
Finansal Bilgiler	Müşteri, Kefil
Hukuki İşlem Bilgileri	Müşteri, Borçlu
Özlük Bilgileri	Çalışan
Performans Bilgileri	Çalışan
Eğitim Bilgileri	Çalışan
Kamera Kayıtları	Çalışan, Ziyaretçi
İşlem Güvenliği Bilgileri	Tüm kullanıcılar
Sağlık Verileri	Çalışan

EK-2 SAKLAMA SÜRELERİ MATRİSİ

Veri Türü	**Saklama Süresi**
Personel Özlük Dosyaları	İş ilişkisinin sona ermesinden itibaren 15 yıl
Bordro ve Ücret Kayıtları	10 yıl
İş Sağlığı ve Güvenliği Kayıtları	15 yıl
İşe Alım Evrakları	2 yıl
Kamera Kayıtları	30 gün - 90 gün
Müşteri Sözleşmeleri	Sözleşme sona erdikten sonra 10 yıl
Muhasebe Belgeleri	10 yıl
MASAK Kapsamındaki Kayıtlar	8 yıl
Log Kayıtları	En az 2 yıl
Ziyaretçi Kayıtları	2 yıl

EK-3 VERİ İHLALİ BİLDİRİM AKIŞI

Aşama 1 – İhlalin Tespiti

↓

Çalışan / Sistem / Tedarikçi tarafından ihlal veya ihlal şüphesi tespit edilir.

↓

Aşama 2 – İlk Bildirim

İlgili yöneticiye ve Bilgi Teknolojileri Birimine derhal bildirim yapılır.

↓

Aşama 3 – Değerlendirme

- İhlalin kapsamı belirlenir.
- Etkilenen veriler tespit edilir.
- Etkilenen kişi sayısı belirlenir.
- Risk analizi yapılır.

↓

Aşama 4 – Müdahale

- Teknik tedbirler uygulanır.
- Erişimler sınırlandırılır.
- Sistem güvenliği sağlanır.

↓

Aşama 5 – Bildirim

Gerekli görülmesi halinde:

- Kişisel Verileri Koruma Kurumu'na,
- İlgili kişilere,
- Yetkili kurumlara

bildirim yapılır.

↓

Aşama 6 – Kapanış ve İyileştirme

- Kök neden analizi yapılır.
- Düzeltici faaliyetler uygulanır.
- Süreç iyileştirilir.
- Kayıtlar arşivlenir.