1) Amaç

Bu politika, LMC MAKİNA SANAYİ VE TİCARET ANONİM ŞIRKETI'nin KVKK m.6 kapsamındaki özel nitelikli kişisel verilerin işlenmesinde yeterli teknik ve idari tedbirleri belirlemek; sistemli, yönetilebilir ve sürdürülebilir bir güvenlik çerçevesi kurmak amacıyla hazırlanmıştır.

2) Dayanak ve İlke

- Hukuki Dayanak: 6698 sayılı KVKK (özellikle m.4, m.6, m.9), ilgili ikincil düzenlemeler ve Kurul kararları/rehberleri.
- Temel İlkeler: Hukuka ve dürüstlük kurallarına uygunluk, doğru ve güncel olma, belirli-açık-meşru amaç, amaçla bağlantılı-sınırlı-ölçülü işleme, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza, güvenlik ve gizlilik.

3) Tanımlar

- Özel Nitelikli Kişisel Veri: KVKK m.6/1'de sayılan veri kategorileri; 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
- İşleyen/Alt İşleyen: Veri sorumlusu adına veri işleyen gerçek/tüzel kişi.
- Maskeleme/Psödönimizasyon: Kişisel verinin kimliği doğrudan ortaya çıkaran unsurlarının ayrıştırılması.
- DPIA (Etki Analizi): İşleme faaliyetinin hak ve özgürlüklere etkisinin sistematik değerlendirilmesi.

4) Kapsamdaki Tipik Özel Nitelikli Veriler

- İK/Personel: İşe giriş/periyodik sağlık raporları, iş kazası kayıtları, engellilik bilgisi, sendika üyeliği bilgisi (varsa), biyometrik turnike/veri (kullanılıyorsa).
- Ziyaretçi ve Tesis Güvenliği: Biyometrik kayıt kullanılmaması esastır; zorunluluk varsa ayrıca DPIA yapılır.
- Müşteri/İş Ortağı (İstisnai): Özel nitelikli veri işlenmesi kural olarak öngörülmez; işlenmesi gerektiğinde bu politika uygulanır.

5) Roller ve Sorumluluklar

((R)Responsible (A)Accountable (C)Consulted (I)Informed Matrisi)

- Üst Yönetim (A/R): Politikayı onaylar; kaynak tahsisi; ihlal yönetimi.
- KVKK Uyum Birimi (R): Politikanın uygulanması, denetim, eğitim, kayıtların tutulması.
- BT Bilgi Güvenliği (R): Erişim kontrolleri, şifreleme, loglama, yedekleme, DLP, SIEM.
- İK (R): Sağlık verileri süreç sahipliği, saklama-imha, yetki matrisi.
- Hukuk (C): Sözleşmeler, aydınlatma, açık rıza, yurtdışı aktarım kurguları.
- İş Birimleri (R): Süreçlere uyum ve kayıt.

HAZIRLAYAN	ONAYLAYAN
İNSAN KAYNAKLARI	GENEL MÜDÜR

- İç Denetim (A/C): Uyum denetimleri ve raporlama.

6) İşleme Şartları ve Aydınlatma

- İşleme Şartı: Özel nitelikli veriler kural olarak açık rıza ile işlenir; kanunda açıkça öngörülmesi veya sağlık-kamu sağlığı/koruyucu hekimlik vb. hallerde m.6/3 istisnaları uygulanır.
- Aydınlatma: İşleme amacı, hukuki sebep, alıcılar, saklama süreleri, haklar açık ve anlaşılır şekilde sunulur.
- Asgari Veri: Amaç için zorunlu olmayan veri toplanmaz.

7) Erişim Yetkilendirme ve Yetki Matrisi

- Rol Tabanlı Erişim (RBAC): Özel nitelikli verilere erişim ihtiyaç-bilmesi gereken prensibi ile sınırlandırılır.
- İki Faktörlü Kimlik Doğrulama: Varlık (sunucu, NAS, DLP konsolu, HRIS) erişimlerinde MFA esastır.
- Yetki İncelemesi: Üç ayda bir erişim hakları gözden geçirilir; görev değişikliği/işten ayrılıkta anlık kapatma.

8) Teknik Tedbirler

- Şifreleme: Dinamik ve durağan veriler için güçlü kriptografi (dinamikte TLS; depolamada AES-256 benzeri). Anahtar yönetimi ayrık kasalarda ya da HSM/KMS.
- Ayrıştırma ve Maskeleme: Operasyon ihtiyaçlarında maskeleme/psödönimizasyon; raporlarda yalın istatistik.
- Loglama ve İzleme: Erişim, okuma, yazma, dışa aktarma loglanır; değiştirilemez formatta saklanır; SIEM korelasyonu.
- Uç Nokta Güvenliği: EDR/anti-malware, tam disk şifreleme, cihaz şifrelemesi, otomatik kilitleme.
- DLP: E-posta/USB/bulut dışa aktarım kontrolü, içerik denetimi, şablon bazlı politikalar.
- Ağ Güvenliği: Segmentasyon (İK ağı ayrı), VPN, firewall, IDS/IPS; uzaktan erişime MFA.
- Yedekleme: 3-2-1 kuralı; yedekler şifreli ve ayrık tutulur; geri-yükleme tatbikatı yılda 1.
- Fiziksel Güvenlik: Sunucu odası, arşiv odası, sağlık dosyaları için kilitli dolap/oda; giriş logları.

9) İdari Tedbirler

- Gizlilik Taahhüdü: Tüm personel ve işleyenler için yazılı taahhüt alınır.
- Eğitim: Çalışanlara ve yeni başlayalanlara eğitim verilir.
- Politika ve Prosedür Seti: Bu politika, Veri İşleme Envanteri, Saklama-İmha Politikası, Veri Sahibi Başvuru Prosedürü, İhlal Müdahale Planı ile birlikte yürür.
- Tedarikçi Yönetimi: İşleyenlerle veri işleme sözleşmesi, teknik-idari tedbir kontrol listesi, yerinde/uzaktan denetim.

HAZIRLAYAN	ONAYLAYAN
İNSAN KAYNAKLARI	GENEL MÜDÜR

10) Saklama, Arşiv ve İmha

- Süreler: Mevzuat (iş sağlığı güvenliği, iş hukuku) ve hak düşürücü zamanlar gözetilir.
- İmha Yöntemleri: Kağıt evrak için mikro-parçalama; elektronik için kriptografik silme/geri döndürülemez silme.
- İmha Kayıtları: Tarih, yöntem, sorumlu kişi, veri kategorisi ve dayanakla kayıt altına alınır.
- Periyodik İmha: En az 6 ayda bir envanter bazlı kontroller.

11) Aktarım (Yurt İçi / Yurt Dışı)

- Yurt İçi: Amaç ve hukuki sebep kapsamında, yetkisiz erişime karşı güvenli yöntemlerle aktarım (şifreli dosya, SFTP, VPN).
- Yurt Dışı: KVKK m.9 çerçevesinde Kurul kararları, yeterlilik mekanizmaları ve/veya ilgili açık rıza şartları gözetilerek yapılır. Şifreli aktarım ve sözleşmesel güvenceler zorunludur.
- E-posta: İçerik şifrelemesi, parola paylaşımı ayrı kanaldan.

12) Sağlık Verileri Yönetimi

- Erişim: İş yeri hekimi ve yetkili İK personeli ile sınırlı; sonuçların gereksiz paylaşımı yasaktır.
- Depolama: Kilitli dolap/ayrı klasör; elektronikse şifreli klasör/ayrı sistem.
- İş Kazası Kayıtları: Sadece mevzuat zorunluluğu kadar; maskeleyerek raporlama.

13) Veri İhlali Müdahale Planı

- Tespit ve Bildirim: Her çalışan şüpheli olayı derhal işverene bildirir.
- İç Değerlendirme; İlk 24 saatte sınıflandırma ve ilk önlemler; 48 saat içinde etki analizi; Kurul bildirimi gecikmeksizin yapılır.
- Delil ve Kayıt: Logların muhafazası, kök neden analizi (Root Cause), düzeltici/önleyici faaliyet (DÖF).
- İlgili Kişi Bildirimi: Etkilenen kişilere makul süre içinde açık ve sade bilgilendirme.

15) Denetim, İzleme ve Raporlama

- İç Denetim: Yılda en az 1; yüksek riskli süreçlerde ara denetimler (örn. biyometri/sağlık verisi).
- KPI'lar: Yetkisiz erişim sayısı, kapatılan açıklar, eğitim katılım oranı, imha periyot uyumu, tedarikçi skorları.
- Yönetim Gözden Geçirmesi: Altı ayda bir; riskler, olaylar, yatırımlar, DÖF durumu.

16) Farkındalık ve Disiplin

- Uygunsuzluk: Politika ihlalleri disiplin prosedürüne tabidir; gerektiğinde sözleşmesel yaptırımlar uygulanır.
- Farkındalık: Tesis içi görseller, e-öğrenme modülleri, phishing simülasyonları.

HAZIRLAYAN	ONAYLAYAN
İNSAN KAYNAKLARI	GENEL MÜDÜR

17) Yürürlük ve Revizyon

Politika yayımlandığı tarihte yürürlüğe girer; değişen mevzuat/iş modeli/teknoloji ile en geç yılda bir gözden geçirilir.

HAZIRLAYAN	ONAYLAYAN
İNSAN KAYNAKLARI	GENEL MÜDÜR