Kişisel Veri Güvenliği Yönetimi Politikası

1. AMAÇ

Bu Politikanın amacı; MABEL MAMAK TURİZM İNŞAAT ÇİÇEKÇİLİK SAĞLIK HİZMETLERİ SANAYİ VE TİCARET A.Ş. nezdinde işlenen kişisel verilerin ve özel nitelikli kişisel verilerin 6698 sayılı Kişisel Verilerin Korunması Kanunu ("KVKK"), ilgili ikincil mevzuat, Kişisel Verileri Koruma Kurulu kararları ve diğer ilgili mevzuata uygun olarak işlenmesini, muhafaza edilmesini, aktarılmasını, güncellenmesini, erişimlerinin sınırlandırılmasını, güvenliğinin sağlanmasını ve saklama süresi sonunda silinmesini, yok edilmesini veya anonim hale getirilmesini sağlamaktır. Bu Politika ile kişisel verilerin hukuka aykırı olarak elde edilmesi, işlenmesi, erişilmesi, aktarılması, ifşa edilmesi, kaybolması, değiştirilmesi veya yetkisiz kişilerce kullanılmasının önlenmesi amaçlanmaktadır.

2. KAPSAM

Bu Politika; MABEL MAMAK TURİZM İNŞAAT ÇİÇEKÇİLİK SAĞLIK HİZMETLERİ SANAYİ VE TİCARET A.Ş. tarafından tamamen veya kısmen otomatik yollarla ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen tüm kişisel verileri kapsar.

Politika; çalışanlar, çalışan adayları, eski çalışanlar, stajyerler, ziyaretçiler, müşteriler, tedarikçiler, alt işveren çalışanları, iş ortakları, hizmet sağlayıcılar ve kişisel verisi işlenen diğer gerçek kişiler bakımından uygulanır.

Politika; dijital sistemler, fiziksel arşivler, basılı belgeler, elektronik posta, taşınabilir medya, kamera kayıtları, insan kaynakları dosyaları, iş sağlığı ve güvenliği kayıtları, muhasebe/finans kayıtları ve kişisel veri içeren tüm iş süreçlerini kapsar.

3. DAYANAK

Bu Politika aşağıdaki mevzuat esas alınarak hazırlanmıştır:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu,
- Veri Sorumluları Sicili Hakkında Yönetmelik,
- Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik,
- Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ,
- Kişisel Verileri Koruma Kurulu kararları, rehberleri ve duyuruları,
- İş Kanunu, İş Sağlığı ve Güvenliği mevzuatı, Türk Ticaret Kanunu ve ilgili diğer mevzuat.

4. TANIMLAR

Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.

Özel nitelikli kişisel veri: KVKK'nın 6. maddesinde sayılan; kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerini ifade eder.

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi ifade eder.

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

Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.

Açık rıza: Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.

5. TEMEL İLKELER

MABEL MAMAK TURİZM İNŞAAT ÇİÇEKÇİLİK SAĞLIK HİZMETLERİ SANAYİ VE TİCARET A.Ş. ,kişisel veri işleme faaliyetlerinde aşağıdaki ilkelere uygun hareket eder:

1. Hukuka ve dürüstlük kurallarına uygun olma,
2. Doğru ve gerektiğinde güncel olma,
3. Belirli, açık ve meşru amaçlar için işlenme,
4. İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,
5. İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme,
6. Gizlilik, bütünlük ve erişilebilirliğin korunması,
7. Yetkisiz erişim, kayıp, ifşa ve kötüye kullanıma karşı uygun teknik ve idari tedbirlerin alınması.

6. KİŞİSEL VERİLERİN İŞLENMESİNE İLİŞKİN ESASLAR

1. Kişisel veriler, KVKK'nın 5. maddesinde düzenlenen işleme şartlarından uygun olanına dayanılarak işlenir; hukuki sebep ve işleme amacı envanterde belgelenir.

2. Özel nitelikli kişisel veriler, KVKK'nın güncel 6. maddesindeki işleme şartlarına uygun olarak ve Kurul tarafından belirlenen yeterli önlemler gözetilerek işlenir.
3. Açık rıza, yalnızca ilgili veri işleme faaliyeti bakımından gerekli olduğu durumlarda alınır. Açık rıza metinleri aydınlatma metinlerinden ayrı düzenlenir.
4. Kişisel veri işleme faaliyetlerinden önce veya en geç veri elde edilmesi sırasında ilgili kişilere KVKK'nın 10. maddesi kapsamında aydınlatma yapılır.
5. Kişisel veriler yalnızca belirli, açık ve meşru amaçlarla işlenir; veri minimizasyonu ilkesi gereğince gereğinden fazla veri toplanmaz.
6. Kişisel verilerin güncelliği, ilgili süreç sahipleri tarafından makul aralıklarla kontrol edilir.
7. Kişisel veriler, işlendikleri amaç için gerekli süre boyunca saklanır; saklama süresi sona erdiğinde silinir, yok edilir veya anonim hale getirilir.

7.KİŞİSEL VERİ İŞLEME ENVANTERİ VE VERBİS

1. Şirket tarafından yürütülen kişisel veri işleme faaliyetleri kişisel veri işleme envanterinde kayıt altına alınır.
2. Envanterde; veri kategorileri, ilgili kişi grupları, işleme amaçları, hukuki sebepler, aktarım alıcı grupları, saklama süreleri ve alınan güvenlik tedbirleri gösterilir.
3. VERBİS yükümlülüğü bulunması halinde, VERBİS kaydı kişisel veri işleme envanteri ile uyumlu şekilde hazırlanır ve güncel tutulur.
4. Mevzuat, organizasyon yapısı veya iş süreçlerinde değişiklik olması halinde envanter ve ilgili kayıtlar güncellenir.

8. İDARİ TEDBİRLER

Şirket, kişisel veri güvenliğini sağlamak amacıyla aşağıdaki idari tedbirleri uygular:

1. KVKK uyum süreçlerinin yürütülmesi için KVKK Komitesi ve Veri Sorumlusu İrtibat Kişisi görevlendirilir.
2. Kişisel veri işleme süreçleri belirlenir, kayıt altına alınır ve periyodik olarak gözden geçirilir.
3. Çalışanlara KVKK, kişisel veri güvenliği, özel nitelikli kişisel veriler ve bilgi güvenliği konularında farkındalık eğitimleri verilir.
4. Kişisel verilere erişim yetkileri görev ve ihtiyaç esasına göre belirlenir.
5. Erişim yetki matrisi oluşturulur ve düzenli aralıklarla gözden geçirilir.
6. Görev değişikliği veya işten ayrılma halinde erişim yetkileri gecikmeksizin kaldırılır veya güncellenir.
7. Çalışanlardan gizlilik ve kişisel veri güvenliği yükümlülüklerine ilişkin taahhüt alınır.
8. Kişisel veri içeren fiziksel dosyalar temiz masa ve temiz ekran kurallarına uygun şekilde korunur.
9. Kişisel veri işleme faaliyetlerinden doğan riskler düzenli olarak değerlendirilir.
10. İç denetimlerde KVKK ve kişisel veri güvenliği kontrollerine yer verilir.
11. Tespit edilen uygunsuzluklar için düzeltici ve önleyici faaliyetler planlanır.

12. Veri işleyenler ve tedarikçilerle yapılan sözleşmelere kişisel verilerin korunmasına ilişkin hükümler eklenir.
13. Veri işleyen hizmet sağlayıcılar risk durumuna göre denetlenebilir veya güvence mekanizmalarına tabi tutulabilir.
14. Kişisel veri güvenliği kurallarına aykırı davranışlar disiplin süreçleri kapsamında değerlendirilir.

9. TEKNİK TEDBİRLER

Şirket, kişisel veri güvenliğini sağlamak amacıyla risk seviyesine uygun teknik tedbirleri alır. Bu kapsamda;

1. Bilgi sistemlerine erişim yetkilendirme esasına göre sınırlandırılır.
2. Kritik sistemlere erişimlerde güçlü parola politikası ve gerekli hallerde çok faktörlü kimlik doğrulama uygulanır.
3. Kullanıcı hesapları kişiye özel tanımlanır; ortak kullanıcı hesabı kullanımından kaçınılır.
4. Kişisel verilere erişim, görüntüleme, değiştirme, silme ve aktarma işlemleri mümkün olduğu ölçüde loglanır.
5. Log kayıtları düzenli olarak kontrol edilir ve güvenli şekilde saklanır.
6. Güvenlik duvarı, antivirüs, zararlı yazılım önleme, ağ güvenliği ve benzeri güvenlik çözümleri risk durumuna göre uygulanır.
7. Sistem, uygulama ve cihazlara ilişkin güvenlik güncellemeleri ve yamalar zamanında yapılır.
8. Kişisel veri içeren sistemlerde risk temelli zafiyet taraması ve gerekli görülen durumlarda sızma testi yapılır; bulguların giderilmesi ve doğrulanması takip edilir.
9. Kişisel verilerin yedeklenmesi sağlanır; yedeklere erişim sınırlandırılır.
10. Veri kaybı, sistem arızası, siber saldırı veya felaket durumlarına karşı iş sürekliliği ve felaket kurtarma tedbirleri uygulanır.
11. Taşınabilir bellek, harici disk ve benzeri cihazların kullanımı kontrol altına alınır.
12. Kişisel verilerin kurum dışına çıkarılması veya harici ortamlara aktarılması ancak yetkili kişilerin onayı ve güvenli aktarım yöntemleri ile yapılabilir.
13. Özel nitelikli kişisel veriler mümkün olduğu ölçüde kriptografik yöntemlerle korunur.
14. Kurumsal cihazların güvenliği, cihazı kullanan çalışan ve ilgili teknik birim tarafından sağlanır.

10. ÖZEL NİTELİKLİ KİŞİSEL VERİLERİN GÜVENLİĞİ

1. Özel nitelikli kişisel veriler "gizli bilgi" niteliğinde değerlendirilir.
2. Özel nitelikli kişisel verilere erişim yalnızca görev gereği erişmesi gereken sınırlı sayıdaki yetkili çalışanlara verilir.
3. Özel nitelikli kişisel verilerin işlendiği birimler, ilgili verilerin gizliliği ve güvenliği konusunda ayrıca bilgilendirilir.
4. Özel nitelikli kişisel veri içeren fiziksel dosyalar kilitli dolaplarda veya kontrollü arşiv alanlarında muhafaza edilir.

5. Özel nitelikli kişisel veri içeren fiziksel belgeler, veri sınıflandırma kurallarına uygun şekilde işaretlenebilir.
6. Özel nitelikli kişisel verilerin elektronik ortamda saklanması halinde erişim yetkileri sınırlandırılır, loglama ve şifreleme gibi uygun güvenlik tedbirleri uygulanır.
7. Özel nitelikli kişisel verilerin aktarımı zorunlu ise güvenli aktarım yöntemleri kullanılır.
8. Sağlık verileri, iş sağlığı ve güvenliği süreçleri ile sınırlı olarak ve yalnızca yetkili kişiler tarafından işlenir.
9. Özel nitelikli kişisel verilerin işlendiği süreçler için ayrıca risk değerlendirmesi yapılır.

11. FİZİKSEL ORTAM GÜVENLİĞİ

1. Kişisel veri içeren fiziki dosyalar, yetkisiz kişilerin erişemeyeceği şekilde muhafaza edilir.
2. Arşiv alanlarına erişim yetkili kişilerle sınırlandırılır.
3. Kişisel veri içeren belgeler masa üzerinde, ortak alanlarda veya herkesin görebileceği şekilde bırakılmaz.
4. Yangın, su baskını, hırsızlık, elektrik kaçağı ve benzeri risklere karşı uygun fiziksel güvenlik önlemleri alınır.
5. Fiziksel ortamda bulunan kişisel veriler, saklama süresi sona erdiğinde güvenli imha yöntemleriyle imha edilir.

12. VERİ AKTARIMI

1. Kişisel veriler, KVKK'da belirtilen işleme ve aktarım şartlarına uygun olarak aktarılır.
2. Veri aktarımı yapılmadan önce aktarım amacı, hukuki sebep, aktarılacak veri kategorisi, alıcı taraf ve aktarım yöntemi değerlendirilir.
3. Kişisel veriler, aktarım amacıyla bağlantılı, sınırlı ve ölçülü olacak şekilde aktarılır.
4. Yurt içi aktarım süreçlerinde gerekli idari ve teknik güvenlik tedbirleri alınır.
5. Yurt dışına kişisel veri aktarımı, KVKK'nın 9. maddesindeki yeterlilik kararı, uygun güvenceler veya istisnai aktarım şartlarından uygulanabilir olanına ve ilgili ikincil mevzuata uygun olarak gerçekleştirilir.
6. E-posta yoluyla kişisel veri aktarımında kurumsal e-posta adresleri kullanılır; gerekli durumlarda şifreleme veya güvenli bağlantı yöntemleri uygulanır.
7. Taşınabilir medya ile aktarım zorunlu ise veri şifrelenir ve aktarım süreci kayıt altına alınır.
8. Kağıt ortamında aktarım yapılacaksa evrakın kaybolması, çalınması veya yetkisiz kişilerce görülmesini önleyecek tedbirler alınır.

13. VERİ İŞLEYENLER VE TEDARİKÇİLER

1. Şirket adına kişisel veri işleyen tedarikçi, alt işveren, hizmet sağlayıcı ve iş ortakları ile yapılan sözleşmelerde kişisel verilerin korunmasına ilişkin hükümlere yer verilir.
2. Veri işleyenler, kişisel verileri yalnızca Şirket'in talimatları ve sözleşmede belirtilen amaçlarla sınırlı olarak işleyebilir.

5. Özel nitelikli kişisel veri içeren fiziksel belgeler, veri sınıflandırma kurallarına uygun şekilde işaretlenebilir.
6. Özel nitelikli kişisel verilerin elektronik ortamda saklanması halinde erişim yetkileri sınırlandırılır, loglama ve şifreleme gibi uygun güvenlik tedbirleri uygulanır.
7. Özel nitelikli kişisel verilerin aktarımı zorunlu ise güvenli aktarım yöntemleri kullanılır.
8. Sağlık verileri, iş sağlığı ve güvenliği süreçleri ile sınırlı olarak ve yalnızca yetkili kişiler tarafından işlenir.
9. Özel nitelikli kişisel verilerin işlendiği süreçler için ayrıca risk değerlendirmesi yapılır.

11. FİZİKSEL ORTAM GÜVENLİĞİ

1. Kişisel veri içeren fiziki dosyalar, yetkisiz kişilerin erişemeyeceği şekilde muhafaza edilir.
2. Arşiv alanlarına erişim yetkili kişilerle sınırlandırılır.
3. Kişisel veri içeren belgeler masa üzerinde, ortak alanlarda veya herkesin görebileceği şekilde bırakılmaz.
4. Yangın, su baskını, hırsızlık, elektrik kaçağı ve benzeri risklere karşı uygun fiziksel güvenlik önlemleri alınır.
5. Fiziksel ortamda bulunan kişisel veriler, saklama süresi sona erdiğinde güvenli imha yöntemleriyle imha edilir.

12. VERİ AKTARIMI

1. Kişisel veriler, KVKK'da belirtilen işleme ve aktarım şartlarına uygun olarak aktarılır.
2. Veri aktarımı yapılmadan önce aktarım amacı, hukuki sebep, aktarılacak veri kategorisi, alıcı taraf ve aktarım yöntemi değerlendirilir.
3. Kişisel veriler, aktarım amacıyla bağlantılı, sınırlı ve ölçülü olacak şekilde aktarılır.
4. Yurt içi aktarım süreçlerinde gerekli idari ve teknik güvenlik tedbirleri alınır.
5. Yurt dışına kişisel veri aktarımı, KVKK'nın 9. maddesindeki yeterlilik kararı, uygun güvenceler veya istisnai aktarım şartlarından uygulanabilir olanına ve ilgili ikincil mevzuata uygun olarak gerçekleştirilir.
6. E-posta yoluyla kişisel veri aktarımında kurumsal e-posta adresleri kullanılır; gerekli durumlarda şifreleme veya güvenli bağlantı yöntemleri uygulanır.
7. Taşınabilir medya ile aktarım zorunlu ise veri şifrelenir ve aktarım süreci kayıt altına alınır.
8. Kağıt ortamında aktarım yapılacaksa evrakın kaybolması, çalınması veya yetkisiz kişilerce görülmesini önleyecek tedbirler alınır.

13. VERİ İŞLEYENLER VE TEDARİKÇİLER

1. Şirket adına kişisel veri işleyen tedarikçi, alt işveren, hizmet sağlayıcı ve iş ortakları ile yapılan sözleşmelerde kişisel verilerin korunmasına ilişkin hükümlere yer verilir.
2. Veri işleyenler, kişisel verileri yalnızca Şirket'in talimatları ve sözleşmede belirtilen amaçlarla sınırlı olarak işleyebilir.

3. Veri işleyenler, kişisel verilerin güvenliği için gerekli teknik ve idari tedbirleri almakla yükümlüdür.
4. Veri işleyenler, kişisel veri ihlali veya ihlal şüphesi halinde Şirket'i gecikmeksizin bilgilendirir.
5. Şirket, gerekli gördüğü durumlarda veri işleyenlerin kişisel veri güvenliği uygulamalarını denetleyebilir veya denetim raporu, taahhüt, sertifika ve benzeri güvence belgeleri talep edebilir.

14. EĞİTİM VE FARKINDALIK

1. Çalışanlara kişisel verilerin korunması, özel nitelikli kişisel verilerin işlenmesi, bilgi güvenliği, temiz masa/temiz ekran, ihlal bildirimi ve veri minimizasyonu konularında eğitim verilir.
2. KVKK Komitesi, Veri Sorumlusu İrtibat Kişisi, İnsan Kaynakları, Bilgi İşlem ve kişisel veri işleme süreçlerinde görev alan personele görev alanlarına uygun ilave eğitimler sağlanabilir.
3. Çalışanlar, kişisel veri güvenliği kuralları hakkında periyodik duyuru, e-posta, bilgilendirme veya pano duyuruları ile bilgilendirilir.
4. Güncel politika, prosedür ve talimatlara çalışanların erişebilmesi sağlanır.

15. İÇ DENETİM VE UYGUNSUZLUK YÖNETİMİ

1. Şirket nezdinde KVKK ve kişisel veri güvenliği süreçleri periyodik olarak gözden geçirilir.
2. İç denetimlerde kişisel veri güvenliği ve KVKK uyumuna ilişkin kontrol sorularına yer verilir.
3. Denetimlerde tespit edilen uygunsuzluklar KVKK Komitesi ve ilgili süreç sahipleri ile paylaşılır.
4. Uygunsuzlukların giderilmesi için düzeltici ve önleyici faaliyetler planlanır.
5. Gerekli görülen hallerde bağımsız üçüncü taraf denetimi yaptırılabilir.
6. Denetim sonuçları üst yönetime raporlanır.

16. KİŞİSEL VERİ İHLALİ YÖNETİMİ

1. Kişisel verilerin hukuka aykırı olarak elde edilmesi, erişilmesi, ifşa edilmesi, değiştirilmesi, kaybolması, silinmesi veya yetkisiz kişilerce kullanılması kişisel veri ihlali olarak değerlendirilir.
2. Çalışanlar, kişisel veri ihlali veya ihlal şüphesi halinde durumu gecikmeksizin Veri Sorumlusu İrtibat Kişisi'ne, KVKK Komitesi'ne veya belirlenen iç bildirim kanalına bildirir.
3. İhlal bildirimi için Bilgi Güvenliği Olay / İhlal Formu kullanılabilir.
4. İhlal şüphesi KVKK Komitesi, Veri Sorumlusu İrtibat Kişisi, Bilgi İşlem, İnsan Kaynakları, hukuk/uyum ve ilgili birimler tarafından değerlendirilir.
5. İhlalin kapsamı, etkilenen kişi grupları, veri kategorileri, risk düzeyi ve alınması gereken önlemler belirlenir.

6. KVKK m.12/5 kapsamında gerekli hallerde Kurula ve etkilenen ilgili kişilere bildirim yapılır; Kurula bildirimde Kurulun belirlediği 72 saatlik süre ve gecikme gerekçelendirme kuralları gözetilir.
7. İhlal sonrasında kök neden analizi yapılır ve tekrarını önleyici tedbirler uygulanır.

17. İLGİLİ KİŞİ BAŞVURULARI

1. İlgili kişiler, KVKK'nın 11. maddesi kapsamındaki haklarını kullanmak üzere Şirket'e başvurabilir.
2. Başvurular; yazılı dilekçe, noter, kayıtlı elektronik posta, güvenli elektronik imza, mobil imza, ilgili kişinin daha önce Şirket'e bildirdiği ve sistemde kayıtlı bulunan e-posta adresi veya Şirket tarafından duyurulan diğer yöntemlerle yapılabilir.
3. Başvurular Veri Sorumlusu İrtibat Kişisi koordinasyonunda değerlendirilir.
4. Başvurular kvkk'nın 13. maddesi uyarınca talebin niteliğine göre en kısa sürede ve en geç otuz gün içinde sonuçlandırılır.
5. Başvurulara verilen cevaplar ve yapılan işlemler kayıt altına alınır.

18. SAKLAMA VE İMHA

1. Kişisel veriler, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilir.
2. Saklama süresi sona eren veya işleme amacı ortadan kalkan kişisel veriler, Kişisel Veri Saklama ve İmha Politikası doğrultusunda silinir, yok edilir veya anonim hale getirilir.
3. İmha işlemleri kayıt altına alınır; imha kayıtları ilgili Yönetmelikte öngörülen asgari süre boyunca muhafaza edilir.
4. Fiziksel ve dijital ortamlarda bulunan kişisel veriler için uygun imha yöntemleri uygulanır.
5. İmha süreçlerinde kişisel verilerin geri döndürülemeyecek ve yetkisiz erişime konu olmayacak şekilde ortadan kaldırılması esas alınır.

19. GİZLİLİK VE DİSİPLİN

1. Çalışanlar, görevleri kapsamında öğrendikleri kişisel verileri ve özel nitelikli kişisel verileri gizli tutmakla yükümlüdür.
2. Gizlilik yükümlülüğü, iş ilişkisinin sona ermesinden sonra da devam eder.
3. Kişisel verilerin hukuka aykırı şekilde işlenmesi, aktarılması, ifşa edilmesi, kopyalanması, silinmesi, değiştirilmesi veya yetkisiz kişilerle paylaşılması halinde şirket içi disiplin süreçleri ve ilgili mevzuat hükümleri uygulanır.
4. Gerekli hallerde hukuki, idari ve cezai süreçler başlatılabilir.

20. SORUMLULUKLAR

20.1. Üst Yönetim

Üst Yönetim; bu Politikanın uygulanması için gerekli organizasyonel desteğin sağlanmasından, politika ve ilgili süreçlerin onaylanmasından, gerekli kaynakların tahsis edilmesinden ve KVKK uyum çalışmalarının desteklenmesinden sorumludur.

20.2. KVKK Komitesi

KVKK Komitesi; kişisel veri güvenliği süreçlerinin koordinasyonundan, politika, prosedür, talimat ve formların hazırlanması ve güncellenmesinden, eğitim ve denetim faaliyetlerinin takip edilmesinden, uygunsuzlukların değerlendirilmesinden ve gerekli iyileştirme faaliyetlerinin üst yönetime raporlanmasından sorumludur.

20.3. Veri Sorumlusu İrtibat Kişisi

Veri Sorumlusu İrtibat Kişisi; ilgili kişi başvurularının koordinasyonundan, Kurum ile yürütülecek iletişim süreçlerinin takibinden, KVKK kayıtlarının güncelliğinin izlenmesinden ve KVKK Komitesi ile koordineli çalışmaktan sorumludur.

20.4. Bilgi İşlem / Bilgi Teknolojileri Birimi

Bilgi İşlem / Bilgi Teknolojileri Birimi; kişisel veri içeren bilgi sistemlerinde erişim kontrolü, loglama, yedekleme, güncelleme, siber güvenlik, şifreleme, zafiyet yönetimi ve teknik güvenlik tedbirlerinin uygulanmasından sorumludur.

20.5. İnsan Kaynakları Birimi

İnsan Kaynakları Birimi; çalışan, çalışan adayı ve stajyer süreçlerinde işlenen kişisel verilerin ve özel nitelikli kişisel verilerin hukuka uygun şekilde alınması, işlenmesi, saklanması, korunması ve gerektiğinde imhası süreçlerinden sorumludur.

20.6. İş Sağlığı ve Güvenliği Süreçlerinden Sorumlu Birimler

İş Sağlığı ve Güvenliği süreçlerinden sorumlu birimler; sağlık verileri başta olmak üzere kendi faaliyet alanlarında işlenen özel nitelikli kişisel verilerin yalnızca yetkili kişilerce işlenmesi, korunması ve gizliliğinin sağlanmasından sorumludur.

20.7. İç Tetkikçiler

İç tetkikçiler; iç denetimlerde KVKK ve kişisel veri güvenliği kontrollerinin yapılmasına destek olmaktan, tespit edilen uygunsuzlukları ilgili birimlere bildirmekten sorumludur.

20.8. Birim Yöneticileri

Birim yöneticileri; kendi sorumluluk alanlarında yürütülen kişisel veri işleme faaliyetlerinin bu Politika'ya uygun yürütülmesini sağlamaktan, çalışanların erişim yetkilerini takip etmekten ve uygunsuzlukları ilgili birimlere bildirmekten sorumludur.

20.9. Tüm Çalışanlar

Tüm çalışanlar; bu Politika'ya, KVKK prosedürlerine, bilgi güvenliği kurallarına, gizlilik yükümlülüklerine ve kendilerine bildirilen talimatlara uygun hareket etmekten sorumludur.

20.10. Veri İşleyenler ve Tedarikçiler

Veri işleyenler ve tedarikçiler; Şirket adına işledikleri kişisel verileri yalnızca sözleşme ve talimatlara uygun şekilde işlemekten, gerekli güvenlik tedbirlerini almaktan ve olası ihlal durumlarını gecikmeksizin Şirket'e bildirmekten sorumludur.