

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. POLİTİKANIN AMACI

Bu politikanın amacı; 6698 sayılı Kişisel Verilerin Korunması Hakkında Kanun'a (Kanun) dayalı olarak çıkarılmış olan ve 30224 sayılı Resmi Gazete 'de 28.10.2017 tarihinde yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in (Yönetmelik) 5. ve 6. maddeleri gereği kişisel verilerin saklanması ve imhasına ilişkin yükümlülüklerin ve Yönetmelik'te belirtilen sair yükümlülüklerin yerine getirilmesi amacı ile **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.** genelinde

2. POLİTİKANIN KAPSAMI

Politika **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.** kişisel verileri ve özel nitelikli kişisel verileri, tüm KVKK Kanunu'nda yer alan düzenlemeler doğrultusunda, **Net Tech Bilişim ve Siber Güvenlik Hizmetleri A.Ş.** tarafından ilişkin olarak kamera ile izlemenin yapıldığı alanların girişlerine söz konusu **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.** çalışanlarını, yöneticilerini, danışanlarını ve kişisel veri paylaşımı söz konusu olan tüm durumlarda iştiraklerini, dış hizmeti sağlayıcılarını ve **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**'nin sair hukuki ilişkiye girdiği gerçek ve tüzel kişileri kapsamaktadır.

Politika Kanun'da belirtildiği şekilde, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla verilerin işlendiği sistemlerde yer alan kişisel verileri kapsamaktadır.

Bu Politikada aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel verilerle beraber genel olarak "Kişisel Veriler"

3. TANIMLAR

Anonim Hale Getirme: Kişisel verilerin başka verilerle eşleştirilse dahi, hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,

İmha: Kişisel verilerin silinmesi, yok (imha) edilmesini,

Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

Kişisel Veri Saklama Tablosu (Süreleri) : Kişisel verilerin NET TECH BİLİŞİM VE SİBER GÜVENLİK

Kişisel Veri İşleme Envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami süreyi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri,

Kişisel Verilerin Silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi,

Kişisel Verilerin Yok (İmha) Edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi,

Özel Nitelikli Kişisel Veri: 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,

Periyodik imha: Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda kişisel verileri saklama ve imha politikasında belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemi,

Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Doğrudan tanımlayıcılar: Tek başlarına, ilişki içinde oldukları kişiyi doğrudan açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,

Dolaylı tanımlayıcılar: Diğer Tanımlayıcılar ile bir araya gelerek ilişki içinde oldukları kişiyi açığa çıkaran, ifşa eden ve ayırt edilebilir kılan tanımlayıcıları,

Kanun: 07.04.2016 tarih ve 29677 sayılı Resmî Gazetede yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanununu,

Yönetmelik: 28.10.2017 tarihli ve 30224 sayılı Resmî Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmeliğini,

Kurul: Kişisel Verileri Koruma Kurulunu,

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

Kişisel Verilerin Korunması ve İşlenmesi Politikası: " <https://www.nettechbilisim.com.tr/tr> " adresinden ulaşılabilecek, **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.** nin elinde bulunan kişisel verilerin yönetilmesine ilişkin usul ve esasları belirleyen politikayı,

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 kapsamına girer.

4.1. KİŞİSEL VERİLERİN SAKLANDIĞI ORTAMLAR

" **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**" nezdinde saklanan kişisel veriler, BGYS (ISO 27001:2013) Kapsamında ilgili verinin niteliğine ve hukuki yükümlülüklerimize uygun bir kayıt ortamında tutulur.

Kişisel verilerin saklanması için kullanılan kayıt ortamları genel itibarıyla aşağıda sayılanlardır. Ancak, bir kısım veriler sahip oldukları özel nitelikler ya da hukuki yükümlülüklerimiz nedeniyle burada gösterilen ortamlardan farklı bir ortamda bulunabilir ve tutulabilir. " **TGRT HABER TV A.Ş.** " veri sorumlusu sıfatıyla hareket etmekte KVK Kanunu'na, Kişisel Verilerin Korunması ve İşlenmesi Politikası'na, işbu Kişisel Veri Saklama ve İmha Politikası'na ve uygun olarak

- a) Matbu ortamlar Verilerin kağıt ya da mikrofilmler üzerine basılarak tutulduğu ortamlardır.
- b) Yerel dijital ortamlar " **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.** bünyesinde yer alan sunucular, sabit ya da taşınabilir diskler, optik diskler gibi sair dijital ortamlardır.
- c) Bulut ortamlar bünyesinde yer almamakla birlikte, " **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**" ın kullanımında olan, kriptografik yöntemlerle şifrelenmiş internet tabanlı sistemlerin kullanıldığı ortamlardır.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

4.2. ORTAMLARIN GÜVENLİĞİNİN SAĞLANMASI

“NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.” kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için ilgili kişisel veri ile tutulduğu ortamın niteliklerine uygun olarak BGYS (ISO 27001:2013) Kapsamında gerekli tüm teknik ve idari tedbirleri almaktadır.

İşbu tedbirler, bunlarla kısıtlı olmamak üzere, ilgili kişisel verinin ve tutulduğu ortamın niteliğine uygun düştüğü ölçüde BGYS (ISO 27001:2013) Kapsamında aşağıdaki idari ve teknik tedbirleri kapsar.

4.2.1. Teknik Tedbirler

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak aşağıdaki teknik tedbirleri almaktadır:

Kişisel verilerin tutulduğu ortamlarda yalnızca teknolojik gelişmelere uygun güncel ve güvenli sistemler kullanılmaktadır, Kişisel verilerin tutulduğu ortamlara yönelik güvenlik sistemleri kullanılmaktadır.

Bilişim sistemleri üzerindeki güvenlik zafiyetlerinin tespitine yönelik güvenlik testleri ve araştırmaları yapılmakta, yapılan test ve araştırmaların sonucunda tespit edilen mevcut ya da muhtemel risk teşkil eden hususlar giderilmektedir.

Kişisel verilerin tutulduğu ortamlara veriye erişim kısıtlanarak yalnızca yetkili kişilerin, kişisel verinin saklanma amacı ile sınırlı olarak bu verilere erişmesine izin verilmektedir.

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş. bünyesinde kişisel verilerin tutulduğu ortamların güvenliğini sağlamak üzere yeterli teknik personel bulundurmaktadır.

4.2.2. İdari Tedbirler

“NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.”, kişisel verilerin saklandığı tüm ortamların ilgili verinin ve verinin tutulduğu ortamın niteliklerine uygun olarak KVKK Kanunu Kapsamında aşağıdaki idari

Kişisel verilere erişimi olan tüm “NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.” çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar yapılmaktadır.

Bilgi güvenliği, özel hayatın gizliliği ve kişisel verilerin korunması alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alınmaktadır.

Kişisel verilerin teknik ya da hukuki gereklilikler nedeniyle üçüncü kişilere aktarılması halinde ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalanmakta, ilgili üçüncü kişilerin bu protokollerdeki

4.2.3. Şirket İçi Denetim

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., Kanun’un 12’nci maddesi uyarınca Kanun hükümlerinin ve işbu Kişisel Veri Saklama ve İmha Politikası ile Kişisel Verilerin Korunması ve İşlenmesi Politikası hükümlerinin uygulanmasına ilişkin KVKK Kanununa uygun şirket içi denetimler yapmaktadır.

Şirket içi denetimler sonucunda bu hükümlerin uygulanmasına ilişkin eksiklik ya da kusurların tespit edilmesi halinde bu eksiklik ya da kusurlar derhal giderilir.

Denetim sırasında ya da sair bir şekilde “NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.” sorumluluğunda bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edildiğinin anlaşılması hâlinde, “NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.” bu durumu en kısa sürede ilgisine ve Kurula bildirir.

5. KİŞİSEL VERİLERİ KORUMA KOMİTESİ’NİN GÖREV VE YETKİLERİ

5.1. Kişisel Verileri Koruma Komitesi Politikanın ilgili iş birimlerine duyurulmasından ve gereklerinin **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.** birimlerince yerine getirilmesinin takibinden sorumludur.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

5.2. Kişisel Verileri Koruma Komitesi kişisel verilerin korunmasına ilişkin mevzuat değişiklikleri, Kurulun düzenleyici işlemleri ile kararları, mahkeme kararları veya süreç, uygulama ve sistemlerdeki değişiklikler gibi durumları ilgili iş birimlerinin takip etmesi ve gerekiyorsa iş süreçlerini güncellemeleri için gerekli duyuruları ve bildirimleri yapar,

5.3. Kişisel Verileri Koruma Komitesi; Kanun ve ikincil düzenlemeleri ile Kurulun kararları ve düzenlemeleri, mahkeme kararları ve sair yetkili makamların kararlarının ve/veya taleplerinin incelenmesi, değerlendirilmesi, takibi ve sonuçlandırılmasına yönelik süreçleri belirler ve ilgili birimlere duyurur.

6. KİŞİSEL VERİLERİN İŞLENME ŞARTLARININ ORTADAN KALKMASI DURUMUNDA YAPILACAKLAR

6.1. Kişisel verilerin işlenmesine yönelik amaç unsurunun ortadan kalkması, açık rızanın geri alınmış olması veya Kanunun 5. ve 6. maddelerinde yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması ya da adı geçen maddelerde istisnalardan hiçbirinin uygulanamayacağı bir durumun söz konusu olması halinde, işleme şartları ortadan kalkan kişisel veriler, ilgili iş birimi tarafından, iş ihtiyaçları göz önüne alınarak, Yönetmeliğin 7., 8., 9. veya 10. maddeleri kapsamında, uygulanan yöntemin gerekçesi de açıklanmak suretiyle silinir, yok (imha) edilir veya anonim hale getirilir. Ancak kesinleşmiş bir mahkeme kararının söz konusu olması halinde mahkeme kararı ile hükmedilen imha yöntemi uygulanmak zorundadır.

6.2. Kişisel veriyi işleyen ya da saklayan tüm kullanıcılar ve veri sahibi “ **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**” birimleri işlemeyle ilgili şartların ortadan kalkıp kalkmadığını en geç dört aylık periyodlar içerisinde, kullandıkları veri kayıt ortamlarında gözden geçireceklerdir. Kişisel veri sahibinin başvurusu ya da Kurulun veya bir mahkemenin bildirimine üzerine, ilgili kullanıcı ve birimler, periyodik denetleme süresine bakmaksızın kullandıkları veri kayıt ortamlarında bu gözden

6.3. Periyodik gözden geçirmeler neticesinde veya herhangi bir anda veri işleme şartlarının ortadan kalkmış olduğu tespit edildiğinde ilgili kullanıcı veya veri sahibi, ilgili kişisel verinin kendi uhdesinde bulunan kayıt ortamından işbu politikaya göre, silinmesine, yok (imha) edilmesine veya anonim hale getirilmesine karar verecektir. Tereddüt duyulan durumlarda ilgili veri sahibi iş biriminden görüş alınarak işlem yapılacaktır. Merkezi Bilgi Sistemlerinde yer alan çok paydaşlı veri sahipliği bulunan kişisel verilerin imhasına yönelik karar alınması gerektiğinde ise Kişisel Verileri Koruma Komitesi'nin görüşü alınacak ve söz konusu kişisel veri hakkında işbu politikaya göre verinin, saklanmasına veya silinmesine, yok (imha) edilmesine veya anonim hale getirilmesine ilgili veri sahibi iş birimi tarafından karar verilecektir.

6.4. Kişisel verilerin silinmesi, yok (imha) edilmesi veya anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır.

6.5. Yönetmeliğin 7.4 maddesi uyarınca, kişisel verilerin silinmesi, yok (imha) edilmesi, anonim hale getirilmesi işlemleriyle ilgili uygulanan yöntemler Politika' nın yürürlüğe girmesinden sonra yayınlanacak ve açıklanacaktır.

6.6. Kişisel verilerin silinmesi, yok (imha) edilmesi veya anonim hale getirilmesinde Kanunun 4. maddesindeki genel ilkeler ile 12. maddesi kapsamında alınması gereken teknik ve idari tedbirlere, ilgili mevzuat hükümlerine, Kurul kararlarına ve mahkeme kararlarına uygun hareket edilmesi zorunludur.

6.7. Bir kişisel verinin sahibi gerçek kişi, Kanunun 13. maddesine istinaden “ **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**.....” 'a başvurarak kendisine ait kişisel verilerin silinmesini, imhasını veya anonim hale getirilmesini talep ettiğinde, ilgili veri sahibi iş birimi, kişisel verileri işleme şartlarının tamamının ortadan kalkıp kalkmadığını inceler. İşleme şartlarının tamamı ortadan kalkmışsa; talebe konu kişisel verileri siler, imha eder veya anonim hale getirir. Bu durumda detayları ISO 27001:203 Bilgi Güvenliği Yönetim Sisteminde Veri İmha Prosedüründe belirlendiği şekilde; talep, başvuru tarihinden itibaren en geç otuz gün içinde sonuçlandırılır ve ilgili kişiye KVKK Sorumlusu tarafından atanan KVKK irtibat sorumlusu aracılığıyla bilgi verilir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu kişisel veriler üçüncü kişilere aktarılmışsa, ilgili veri sahibi iş birimi bu durumu derhal aktarım yapılan üçüncü

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

6.8. Kişisel verileri işleme şartlarının tamamının ortadan kalkmadığı durumlarda, kişisel veri sahiplerinin verilerinin silinmesi veya imha edilmesine yönelik talepleri “**NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**” tarafından Kanunun 13. maddesinin 3. fıkrası uyarınca gerekçesi açıklanarak reddedilebilir. Ret cevabı ilgili kişiye en geç 30 gün içerisinde yazılı olarak ya da elektronik ortamda bildirilir.

6.9. Kişisel verilerin silinmesi ya da imha edilmesine yönelik talepler ancak ilgili kişinin kimlik tespitinin yapılmış olması kaydıyla değerlendirilecektir. Söz konusu kanallar dışında yapılacak taleplerde ilgili kişiler kimlik tespitinin yada doğrulamasının yapılabileceği kanallara yönlendirilecektir.

7. POLİTİKANIN YÜRÜRLÜĞE SOKULMASI, İHLAL DURUMLARI VE YAPTIRIMLAR

7.1. İşbu Politika tüm çalışanlara ve Kişisel veri sahiplerine “ **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**” İnternet sitesinden duyurularak yürürlüğe girecek ve yürürlüğü itibarıyla tüm iş birimleri, danışmanlar, müşteriler, sigorta şirketleri, dış hizmet sağlayıcıları ve sair **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.** “ nezdinde kişisel veri

7.2. “ **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**” çalışanlarının Politikanın gereklerini yerine getirip getirmediğinin takibi ilgili çalışanların amirlerinin sorumluluğunda olacaktır. Politikaya aykırı davranış tespit edildiğinde konu derhal ilgili çalışanın amiri tarafından bağlı bulunan bir üst amire bildirilecektir. Aykırılığın önemli boyutta olması

7.3. Politikaya aykırı davranan çalışan hakkında, İnsan Kaynakları tarafından yapılacak değerlendirme sonrasında gerekli idari işlem yapılacaktır.

7.4. Politika gereklerinin yerine getirilmesi için “ **TGRT HABER TV A.Ş.**” tarafından; KVKK Kanunu Kapsamında gerekli tüm güvenlik önlemleri alınmaktadır.

8. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜREÇLERİNDE YER ALACAK KİŞİLER VE SORUMLULUKLARI

“ **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.** içerisinde Kanun, Yönetmelik ve Politika ile belirtilen verinin imhasına dair gereklerin yerine getirilmesinde tüm çalışanlar, müşteriler, sigorta şirketleri, danışmanlar, dış hizmet sağlayıcıları ve sair surette “ **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**” nezdinde kişisel veri saklayan ve işleyen herkes bu gerekleri yerine getirmekten sorumludur.

Her iş birimi kendi iş süreçlerinde ürettiği veriyi saklamak ve korumakla yükümlüdür; ancak üretilen verinin iş biriminin kontrolü ve yetkisi dışında sadece bilgi sistemlerinde bulunması durumunda, söz konusu veri bilgi sistemlerinden sorumlu birimler tarafından saklanacaktır.

İş süreçlerini etkileyecek ve veri bütünlüğünün bozulmasına, veri kaybına ve yasal düzenlemelere aykırı sonuçlar

8.1. KİŞİSEL VERİLERİ KORUMA KOMİTESİ

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş. bünyesinde bir Kişisel Verileri Koruma Komitesi kurar. Kişisel Verileri Koruma Komitesi, ilgili kişilerin verilerinin hukuka, Kişisel Verilerin Korunması ve İşlenmesi Politikasına ve Kişisel Veri Saklama ve İmha Politikasına uygun olarak saklanması ve işlenmesi için gerekli işlemleri yapmak/yaptırmak ve süreçleri denetlemekle yetkili ve görevlidir.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Kişisel Verileri Koruma Komitesi bir yönetici, bir idari uzman ve bir teknik uzman olmak üzere en az üç kişiden oluşur. Kişisel Veri Komitesinde görevli “ **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**” çalışanlarının unvanları ve görev tanımları

Unvan	Görev Tanımı
Kişisel Verileri Koruma Komitesi Yöneticisi	Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; Kanun, Kişisel Verilerin Korunması ve İşlenmesi Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür.
KVK Uzmanı (İrtibat Sorumlusu) (Teknik ve İdari)	İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Komitesi Yöneticisine raporlanmasından; Kişisel Veri Komitesi Yöneticisi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Komitesi Yöneticisinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Komitesi Yöneticisine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur.

8.2. SAKLAMA VE İMHA NEDENLERİ

8.2.1. Saklama Nedenleri

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş. bünyesinde tutulan kişisel veriler Kanun ve Kişisel Veriler Politikamız (ilgili politikaya [https:// www.nettechbilisim.com.tr/tr](https://www.nettechbilisim.com.tr/tr)) adresinden ulaşabilirsiniz) uyarınca, burada belirtilen amaç ve nedenlerle saklanmaktadır.

8.2.2. İmha Nedenleri

“ **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**” bünyesinde bulunan kişisel veriler ilgili kişinin talebi halinde ya da Kanun’un 5’nci ve 6’ncı maddelerinde sayılan nedenlerin ortadan kalkması halinde resen işbu imha politikası uyarınca silinir, yok (imha)

ibarettir:

1. Kanunlarda açıkça öngörülmesi.
2. Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.
3. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.
4. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.
5. İlgili kişinin kendisi tarafından alenileştirilmiş olması.
6. Bir hakkın tesisi, kullanılması veya korunması için veri işleminin zorunlu olması.
7. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

8.3. İMHA YÖNTEMLERİ “

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş..... “, Kanuna ve sair mevzuatı ile Kişisel Verilerin Korunması ve İşlenmesi Politikasına

uygun olarak sakladığı kişisel verileri, verilerin işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde ilgili kişinin talebi doğrultusunda ya da işbu Kişisel Veri Saklama ve İmha Politikasında belirtilen süreler içinde re’sen siler, yok (imha) eder veya anonim hale getirir.

“ **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.**“ tarafından en çok kullanılan silme, yok etme ve anonim

8.3.1.1 Silme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri

Karartma

Matbu ortamda bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin, mümkün olan durumlarda kesilmesi, mümkün olmayan durumlarda ise geri döndürülemez ve teknolojik çözümlerle okunamayacak şekilde sabit mürekkep kullanılarak görünmez hale getirilmesi şeklinde yapılır.

Bulut ve Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Silme Yöntemleri

Yazılımdan güvenli olarak silme

Bulut ortamda ya da yerel dijital ortamlarda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir. Bu şekilde silinen verilere tekrar ulaşılamaz.

8.3.1.2 Yok (imha) Etme Yöntemleri

Matbu Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri

Fiziksel yok etme

Matbu ortamda tutulan belgeler evrak imha makineleri ile tekrar bir araya getirilemeyecek şekilde yok edilir.

Yerel Dijital Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri

Fiziksel yok etme

Kişisel veri barındıran optik ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek, fiziksel olarak kesmek ve/veya delmek ya da bir metal öğütücünden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır.

De-manyetize etme (degauss)

Manyetik medyanın yüksek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Üzerine yazma

Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazılarak eski verinin okunmasının ve kurtarılmasının önüne geçilir.

Bulut Ortamda Tutulan Kişisel Veriler İçin Yok Etme Yöntemleri

Yazılımdan güvenli olarak silme

Bulut ortamda tutulan kişisel veriler bir daha kurtarılamayacak şekilde dijital komutla silinir ve bulut bilişim hizmet ilişkisi sona erdiğinde kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir. Bu şekilde silinen verilere tekrar ulaşılamaz.

8.3.1.3. Anonimleştirme Yöntemleri

Anonimleştirme, kişisel verilerin başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

Değişkenleri çıkarma	<p>İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da bir kaçının çıkarılmasıdır.</p> <p>Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabilmesi gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir.</p>
Bölgesel gizleme	<p>Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumunda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir.</p>
Genelleştirme	<p>Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiksel veri haline getirilmesi işlemidir.</p>
Alt ve üst sınır kodlama / Global kodlama	<p>Belli bir değişken için o değişkene ait aralıklar tanımlanarak kategorilendirilir. Değişken sayısal bir değer içermiyorsa bu halde değişken içindeki birbirine yakın veriler kategorilendirilir.</p> <p>Aynı kategori içinde kalan değerler birleştirilir.</p>
Mikro birleştirilme	<p>Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Bu sayede veri içerisinde bulunan dolaylı tanımlayıcılar bozulmuş olduğundan, verinin ilgili kişiyle ilişkilendirilmesi zorlaştırılır.</p>

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Veri karma ve bozma Kişisel veri içerisindeki doğrudan ya da dolaylı tanımlayıcılar başka değerlerle karıştırılarak ya da bozularak ilgili kişi ile ilişkisi koparılır ve tanımlayıcı niteliklerini kaybetmeleri sağlanır.

“NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.”, kişisel verilerin anonim hale getirilmesi için ilgili verinin niteliğine göre bu sayılan anonimleştirme yöntemlerinden bir ya da birkaçını kullanır. NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., bu anonimleştirme yöntemlerini kullanırken K-Anonimlik, L-Çeşitlilik ve T-Yakınlık istatistik yöntemlerini kullanabilir.

9. KİŞİSEL VERİLERİ SAKLAMA VE İMHA SÜRELERİ

Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo Ek: 1’de yer almaktadır. Periyodik imha ya da talep üzerine gerçekleştirilecek imha işlemlerinde söz konusu saklama ve imha süreleri dikkate alınacaktır. Kişisel Verileri Saklama ve İmha Sürelerini Gösteren Tablo NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş. kişisel veri envanterinde yer alacak süreçlerin sahibi iş birimlerince, tereddüt halinde Kişisel Verileri Koruma Komitesi değerlendirmeleri de alınarak, güncellenecektir.

9.1. Kişisel veri Saklama Tablosu (Süreleri)

VERİ SAHİBİ	VERİ KATEGORİSİ	VERİ SAKLAMA SÜRESİ
Çalışan	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri	Hizmet akdinin devamında ve hitamından itibaren de 50(elli) yıl müddetle muhafaza edilir.
Çalışan	İşe alım evrakları ile Sosyal Güvenlik Kurumuna gerçekleştirilen; hizmet süresine ve ücrete dair bildirimlere esas özlük verileri dışında kalan özlük verileri	Hizmet akdinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 10(on) yıl müddetle muhafaza edilir.
Çalışan	İşyeri Kişisel Sağlık Dosyası İçeriğindeki Veriler	Hizmet akdinin devamında ve hitamından itibaren 30(otuz) yıl müddetle muhafaza edilir.
İş Ortağı/Çözüm Ortağı/Danışman	İş Ortağı/Çözüm Ortağı/Danışman ile “” arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, İş Ortağı/Çözüm Ortağı/Danışman çalışanı verileri	İş Ortağı/Çözüm Ortağı/Danışmanın, “”la olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu Md.146 ile Türk Ticaret Kanunu M.82 uyarınca 10(on) yıl süre ile saklanır.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Ziyaretçi	“.....”a ait fiziki mekana girişte alınan Ziyaretçi'ye ait ad, soyad, T.C.K.N., araç plakası ile kamera kayıtları, telefon aramalarında alınan ses kayıtları	2(iki) yıl süre ile saklanır.
İnternet Sitesi Ziyaretçisi	İnternet Sitesi Ziyaretçisi'ne ait ad, soyad, e-posta adresi, gezinme hareketleri bilgileri	2(iki) yıl süre ile saklanır.
Çalışan Adayı	Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler	En fazla 2(iki) yıl olmak üzere özgeçmişin güncelliğini kaybedeceği süre kadar saklanır.
Stajyer(öğrenci)	Stajyer'e ait staj dosyasında yer alan bilgiler	Staj ilişkisinin devamında ve hitamını takip eden takvim yılı yılbaşından itibaren de 10(on) yıl müddetle muhafaza edilir.
Müşteri	Müşteri'ye ait ad, soyad, T.C.K.N., iletişim bilgileri, ödeme bilgileri ve yöntemleri, gezinme hareketleri bilgileri, telefon aramalarında alınan ses kayıtları, ürün/hizmet tercihleri, işlem geçmişi, özel gün bilgileri	Müşteri'nin, satın almış olduğu her bir ürün/hizmetin sunulmasından itibaren Türk Borçlar Kanunu Md.146 ile Türk Ticaret Kanunu Md.82 uyarınca 10(on) yıl süre ile saklanır.
Müşteri	Kamera görüntüleri, araç plaka bilgisi	2(iki) yıl süre ile saklanır.
Potansiyel Müşteri	Potansiyel Müşteri ile NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş. arasındaki ticari ilişki kurulmasına dair sözleşme görüşmeleri sırasında alınan kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon	2(iki) yıl süre ile saklanır.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

“ NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.” nın İşbirliği içinde Olduğu Kurum/ ... (Tedarikçi, Fason Üretici,	“.....”ın İşbirliği içinde Olduğu Kurum/Firmalar ile “.....” arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon aramalarında alınan ses kayıtları, “.....”ın İşbirliği içinde Olduğu Kurum/Firma çalışanı verileri	“.....”ın İşbirliği içinde Olduğu Kurum/Firmaların, “.....”la olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu Md.146 ile Türk Ticaret Kanunu Md.82 uyarınca 10(on) yıl süre ile saklanır.
---	--	---

* Mevzuat uyarınca daha uzun bir süre düzenlenmiş olması ya da mevzuat uyarınca zamanaşımı, hak düşürücü süre, saklama süreleri vb. için daha uzun bir süre öngörülmüş olması halinde, mevzuat hükümlerindeki süreler azami saklama süresi olarak kabul edilir.

3.3.2. İmha Süreleri

“ NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.”, Kanun, ilgili mevzuat, Kişisel Verilerin Korunması ve İşlenmesi Politikası ve işbu Kişisel Verileri Saklama ve İmha Politikası uyarınca sorumlu olduğu kişisel verileri silme, yok (imha) etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işlemi, kişisel verileri siler, yok eder veya anonim hale getirir.

İlgili kişi, Kanunun 13’ncü maddesine istinaden “ NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.”a başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

1. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; “ NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.” talebi konu kişisel verileri talebi aldığı günden itibaren 30 (otuz) gün içinde gerekçesini açıklayarak uygun imha yöntemi ile siler, yok eder veya anonim hale getirir. “ NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.”ın talebi almış sayılması için ilgili kişinin talebini Kişisel Verilerin Korunması ve İşlenmesi Politikasına uygun olarak yapmış olması gerekir. “ NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.”, her halde
2. Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep “ NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.” tarafından Kanunun 13’ncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

10. PERİYODİK İMHA SÜRELERİ

6698 sayılı KVKK Kanununda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda; “ NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.” işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re’sen gerçekleştirilecek bir işlemle siler, yok (imha) eder veya anonim hale getirir.

10.1. İMHA İŞLEMİNİN HUKUKA UYGUNLUĞUNUN DENETİMİ

“ NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.”, gerek talep üzerine gerekse periyodik imha süreçlerinde re’sen gerçekleştirdiği imha işlemlerini Kanuna, sair mevzuata, Kişisel Verilerin Korunması ve İşlenmesi Politikasına ve işbu

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., imha işlemlerinin bu düzenlemelere uygun olarak yapıldığını temin etmek amacıyla bir takım idari ve teknik tedbirler almaktadır.

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., işbu politikada yer alan her bir imha yöntemine uygun teknik araç ve ekipman temin eder.

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., imha işlemlerinin yapıldığı yerin güvenliğini sağlar.

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., imha işlemi yapan kişilerin erişim kayıtlarını tutar.

10.1.2. İdari Tedbirler

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., imha işlemi yapacak çalışanlarının bilgi güvenliği, kişisel veriler ve özel hayatın gizliliği konularında farkındalıklarının artırılması ve bilinçlendirilmesi için çalışmalar

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., bilgi güvenliği, özel hayatın gizliliği, kişisel verilerin korunması ve güvenli imha teknikleri alanındaki gelişmeleri takip etmek ve gerekli aksiyonları almak üzere hukuki ve teknik danışmanlık hizmeti alır.

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., teknik ya da hukuki gereklilikler nedeniyle imha işlemi üçüncü kişilere yaptırdığı durumlarda ilgili üçüncü kişilerle kişisel verilerin korunması amacıyla protokoller imzalar, ilgili üçüncü kişilerin bu protokollerdeki yükümlülüklerine uyması için gerekli tüm özeni gösterir.

Kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan bütün işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az üç yıl süreyle saklanır

11. YÜRÜRLÜK

11.1. Politika yayınlanma tarihi itibari ile yürürlüğe girecektir.

11.2. Politikanın **NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş.** genelinde duyurulması ve gerekli güncellemelerin yapılması Kişisel

Verileri Koruma Komitesi'nin sorumluluğundadır.

12. GÜNCELLEME ve UYUM

NET TECH BİLİŞİM VE SİBER GÜVENLİK HİZMETLERİ A.Ş., Kanunda yapılan değişiklikler nedeniyle, Kurum kararları uyarınca ya da sektördeki ya da bilişim alanındaki gelişmeler doğrultusunda, Kişisel Verilerin Korunması ve İşlenmesi Politikasında ya da işbu Kişisel Veri Saklama ve İmha Politikasında değişiklik yapma hakkını saklı tutar.