1. AMAÇ

Bu Politikanın amacı, PTT AŞ'nin işlem süreçleri kapsamında; 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili ikincil mevzuata uygun olarak işlenen kişisel verilerin hukuka uygun olarak saklanması ve imha edilmesi açısından benimsenen esas ve usulleri düzenlemektir.

2. KAPSAM

İşbu Politika; müşteri, müşteri adayı, personel, personel adayı, ziyaretçi, katılımcı, iş ve çözüm ortağı, hissedarı veya personeli gibi veri sahibi ilgili kişilerin PTT AŞ tarafından işlenen tüm kişisel verilerinin saklanmasına ve DHU.PL02 Saklama Süreli Standart Dosya Planı'na göre saklama süresi sona erenlerin re'sen imhasına ilişkin tüm ortam ve süreçleri kapsar.

3. DAYANAK

Bu politika 6698 sayılı Kişisel Verilerin Korunması Kanunu ve alt mevzuatına dayalı olarak hazırlanmıştır.

4. TANIMLAR VE KISALTMALAR

4.1 Açık Rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızadır.

4.2 Alıcı Grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisidir.

4.3 Birim: PTT AŞ bünyesindeki Kurul/Komite, Başkanlık, Müşavirlik, Daire Başkanlığı, Birimler, Özel Kalem Müdürlüğü ve Başmüdürlükleri ifade eder.

4.4 Birim Arşivi: Kamu kurum ve kuruluşlarında yapılan iş ve işlemler, haberleşmeler ile gerçek veya tüzel kişilerin gördükleri hizmetler neticesinde oluşan, güncelliğini kaybetmemiş olarak aktif bir biçimde ve günlük iş akışı içinde işlevi bulunan ve kullanılan belgelerin ilgili birimlerince belirli bir süre saklandığı arşivdir.

4.5 BELGENET: Elektronik Belge Yönetimi Sistemi'dir.

4.6 Elektronik Ortam: Kişisel verilerin elektronik aygıtlar ile oluşturulabildiği, okunabildiği, değiştirilebildiği ve yazılabildiği ortamlardır.

4.7 Elektronik Olmayan Ortam: Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlardır.

4.8 İlgili Kişi: Kişisel verisi işlenen gerçek kişidir.

4.9 İlgili Kullanıcı: 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 kişilerdir.

4.10 İmha: Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir.

4.11. İrtibat Kişisi: Türkiye'de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye'de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kişisel Verileri Koruma Kurumu ile iletişimi sağlamak amacıyla Veri Sorumluları Siciline kayıt esnasında bildirilen gerçek kişidir.

4.12 Kanun: 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur.

4.13 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 ortamdır.

4.14 Kişisel Veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.

4.15 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 envanterdir.

4.16 Kişisel Verilerin İşlenmesi: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, saklanması, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemdir.

4.17 Kişisel Verilerin Anonim Hale Getirilmesi: Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

4.18 Kişisel Verilerin Silinmesi: Kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

4.19 Kişisel Verilerin Yok Edilmesi: Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

4.20 Kurul: Kişisel Verileri Koruma Kurulu'dur.

4.21 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 verileridir.

4.22 Periyodik İmha: Kanunda yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda RYB.PK02 Kişisel Verileri Saklama ve İmha Politikasında belirtilen ve tekrar eden aralıklarla re'sen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemidir.

4.23 Politika: İşbu RYB.PK02 Kişisel Verileri Saklama ve İmha Politikası'dır.

4.24 Şirket/PTT AŞ: Posta ve Telgraf Teşkilatı Anonim Şirketi'dir.

4.25 Taşra Teşkilatı: Şirketin Genel Müdürlük Birimleri dışındaki tüm birimleridir.

4.26 Veri Kayıt Sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

4.27 Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasında ve yönetilmesinden sorumlu gerçek veya tüzel kişidir.

4.28 Veri Sorumluları Sicil Bilgi Sistemi (VERBİS): Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kişisel Verileri Koruma Kurumu Başkanlığı tarafından oluşturulan ve yönetilen bilişim sistemidir.

4.29 Yönetmelik: Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'tir.

"Bu dokümanın güncelliği, elektronik ortamda EYS Yazılımından takip edilmelidir. Basılı kopyalar "Kontrolsüz Kopyadır."

5. SORUMLULUKLAR

PTT AŞ'nin tüm birimleri ve personeli, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, personelin eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1: Kişisel Verilerin Saklama ve İmha Süreçlerinde Görev Dağılımı

ÜNVAN	BİRİM	GÖREV
Birim Sorumlusu	Risk Yönetimi Birimi	Kişisel verilerin korunması açısından PTT AŞ'nin İrtibat Kişisi olarak Kişisel Verileri Koruma Kurumu ile PTT AŞ arasındaki iletişimin sağlanmasından ve PTT AŞ bünyesinde Kanuna uyum çalışmalarının yürütülmesinden sorumludur.
PTT AŞ tüm Başkan/Müşavir/Daire Başkanı/Birim Sorumlusu	Tüm Başkanlık/Müşavirlik/Daire Başkanlığı/Birimler	Başkanlık/Müşavirlik/Daire Başkanlığı/Birimler görev kapsamına giren faaliyet konularında işbu Politikaya uygunluğun sağlanmasından sorumludur.
Başmüdür	Başmüdürlük	PTT AŞ Taşra Teşkilatı görev kapsamına giren faaliyet konularında işbu Politika'ya uygunluğun sağlanmasından sorumludur.

6. UYGULAMA

6.1 Kayıt Ortamları

Kişisel veriler, aşağıda Tablo 2'de sayılan elektronik ve elektronik olmayan ortamlarda, hukuka uygun ve güvenli bir şekilde saklanır.

"Bu dokümanın güncelliği, elektronik ortamda EYS Yazılımından takip edilmelidir. Basılı kopyalar "Kontrolsüz Kopyadır."

Tablo 2: Kişisel Verilerin Kayıt Ortamları

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
a) Sunucular (Etki alanı, yedekleme, e-posta, veritabanı, web, dosya paylaşım, vb.) b) Yazılımlar (ofis yazılımları, portal, BELGENET, VERBİS vb.) c) Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, antivirüs vb.) ç) Kişisel bilgisayarlar (Masaüstü, dizüstü) d) Mobil cihazlar (telefon, tablet vb.) e) Optik diskler (CD, DVD vb.) f) Çıkartılabilir bellekler (USB, Hafıza Kart vb.) g) Yazıcı, tarayıcı, fotokopi makinesi.	a) Kâğıt, b) Manuel Veri Kayıt Ortamları (Sözleşmeler ve fer'i dokümanları, ziyaretçi kayıt defterleri, gönderici-alıcı formları, anket formları, dilekçeler vb.), c) Yazılı, basılı, görsel ortamlar.

6.2 Saklama

6.2.1 Saklamayı Gerektiren Hukuki Sebepler

RYB.TB01 Kişisel Verilerin Saklanmasını Gerektiren Hukuki Sebepler Tablosunda yer almaktadır.

6.2.2 Saklamayı Gerektiren Diğer Sebepler

PTT AŞ işlem süreçleri kapsamında işlenen kişisel verilerin saklanma amaçları aşağıda sayılmaktadır.

a) Kanundan doğan yükümlülüklerin yerine getirilmesi,

b) PTT AŞ tarafından yürütülen faaliyet ve süreçler ile üstlenilen görevlerin icrası,

c) İletişim sağlanması,

ç) İş/Çözüm Ortakları ile ilişkilerin ve faaliyetlerin yürütülmesi,

d) Mali/Finansal süreçlerin yönetilmesi,

e) Doğmuş veya doğabilecek hukuki/cezai/idari uyuşmazlıkların takibi ve ispat külfetinin yerine getirilmesi,

f) Kurumsal sosyal sorumluluk projelerinin yerine getirilmesi,

g) İstihdam edilenlere karşı yükümlülüklerin yerine getirilmesi,

ğ) PTT AŞ içi denetimlerin sağlanması,

h) Yapılan iş ve işlemlerin takibi, analiz ve raporlanması,

ı) İstatistiksel çalışmalar yapılması,

i) Müşteri ilişkilerinin yönetilmesi,

"Bu dokümanın güncelliği, elektronik ortamda EYS Yazılımından takip edilmelidir. Basılı kopyalar "Kontrolsüz Kopyadır."

j) Müşteri memnuniyeti süreçlerinin yönetilmesi,

k) Ziyaretçi ve toplantı kayıtlarının tutulması,

l) Reklam faaliyetlerinin yürütülmesi,

m) CİMER, Bilgi Edinme Dilekçesi, PTT AŞ'ye ait INFO sistemi veya çağrı merkezi aracılığıyla gelen öneri, talep ve şikayetlerin sonuçlandırılması.

6.3 İmha

6.3.1 İmhayı Gerektiren Durumlar

Aşağıda belirtilen hallerde kişisel veriler imha edilir.

a) İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,

b) İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,

c) Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,

ç) Kanunun 11. maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi veya yok edilmesine ilişkin yaptığı başvurunun PTT AŞ tarafından kabul edilmesi,

d) PTT AŞ'nin, ilgili kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,

e) Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması.

6.3.2 İmha Teknikleri

6.3.2.1 İlgili mevzuatta öngörülen süre ya da işlendikleri amaç için gerekli olan saklama süresinin sonunda kişisel veriler, PTT AŞ tarafından re'sen veya ilgili kişinin başvurusu üzerine yine ilgili mevzuat hükümlerine uygun olarak aşağıda belirtilen tekniklerle imha edilir.

6.3.2.2 Kişisel Verilerin Silinmesi

PTT AŞ tarafından kullanılabilecek silme teknikleri aşağıdaki Tablo 3'te açıklanmaktadır.

Tablo 3: Kişisel Verilerin Silinmesi Teknikleri

Veri Kayıt Ortamı	Açıklama
Sunucu Sistemlerinde Yer Alan Kişisel Veriler	Sunucu sistemlerinde yer alan kişisel verilerden, saklama süresi sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.

"Bu dokümanın güncelliği, elektronik ortamda EYS Yazılımından takip edilmelidir. Basılı kopyalar "Kontrolsüz Kopyadır."

Veri Tabanlarında Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklama süresi sona erenler, veri tabanı yöneticisi hariç diğer kullanıcılar ve uygulamalar için hiçbir şekilde erişilemez hale getirilir.
Fiziksel Ortamda Yer Alan Kişisel Veriler	Fiziksel ortamda tutulan kişisel verilerden DHU.PL02 Saklama Süreli Standart Dosya Planı'na göre saklama süresi sona erenler 6 (altı) ay içerisinde re'sen silinir. Kağıt ortamında bulunan kişisel veriler karartma yöntemi kullanılarak silinir. Karartma 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 yapılır.
Taşınabilir Medyada Bulunan Kişisel Veriler	Flash tabanlı sistemlerde kişisel veri tutulması yasaktır.

6.3.2.3 Kişisel Verilerin Yok Edilmesi

PTT AŞ tarafından kullanılabilecek yok etme teknikleri aşağıdaki Tablo 4'te açıklanmaktadır.

Tablo 4: Kişisel Verilerin Yok Edilmesi Teknikleri

Veri Kayıt Ortamı	Açıklama
Fiziksel Ortamda Yer Alan Kişisel Veriler	Kâğıt ortamında yer alan kişisel verilerden, DHU.PL02 Saklama Süreli Standart Dosya Planı'na göre saklama süresi sona erenler re'sen yok edilir. Kâğıt ortamında yer alan kişisel verilerden saklama süresi sona erenler, kâğıt kırpma makinelerinde, mümkün olmadığı takdirde kesici araç gereçlerle yeterince tahrip edilerek, anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölünerek yok edilir.

"Bu dokümanın güncelliği, elektronik ortamda EYS Yazılımından takip edilmelidir. Basılı kopyalar "Kontrolsüz Kopyadır."

Disk Sistemlerinde, Optik/Manyetik Medyada Yer Alan Kişisel Veriler	Optik medya ve manyetik medyada yer alan kişisel verilerden saklama süresi sona erenlerin küçük parçalara ayırılacak şekilde kırılması, eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medyanın özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

6.3.2.4 Kişisel Verilerin Anonim Hale Getirilmesi

PTT AŞ tarafından, kişisel veriler hakkında; değişkenleri çıkartma, kayıtları çıkartma, alt ve üst sınır kodlama, bölgesel gizleme, örnekleme, mikro birleştirme, K anonimlik, L çeşitlilik, T çeşitlilik gibi teknikler kullanılır.

6.4 Saklama ve İmha Süreleri

Saklama süreleri süreç, evrak ve işlem bazlı olarak PTT AŞ'nin tabi olduğu kanun ve ikincil mevzuat gereğince, Devlet Arşivleri Yönetmeliğine uygun olarak hazırlanan DHU.PL02 Saklama Süreli Standart Dosya Planı'nda, muhtelif şekillerde belirlenmiştir.

6.5 Periyodik İmha Süresi

Yönetmelik'in 11. maddesi gereğince PTT AŞ, periyodik imha süresini 6 (altı) ay olarak belirlemiştir. Buna göre, PTT AŞ'de, her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

6.6 Kişisel Verilerin Hukuka Uygun Olarak Saklanmasını ve İmha Edilmesini Sağlamak Üzere Alınan Teknik ve İdari Tedbirler

Kişisel verilerin hukuka uygun olarak; işlenmesini, saklamasını ve imha edilmesini sağlamak üzere; gerek Kanun ve ikincil mevzuat hükümleri, gerekse Kurul kararları ve rehberleri uyarınca alınması gereken teknik ve idari tedbirler alınarak kişisel verilerin hukuka uygun şekilde korunması sağlanır.

6.6.1 Teknik Tedbirler

6.6.1.1 Sızma (Penetrasyon) testleri ile PTT AŞ'nin bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınır.

6.6.1.2 Bilgi güvenliği ihlal olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenir.

6.6.1.3 Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim ve kullanıcıların yetkilendirilmesi (erişim ve yetki matrisi) ile kişisel verilerin işlenmesi sınırlandırılır.

6.6.1.4 PTT AŞ'nin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınır.

6.6.1.5 Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi, 7/24 çalışan izleme sistemi, yerel alan ağını oluşturan kenar anahtarların fiziksel güvenliğinin sağlanması, yangın söndürme sistemi, iklimlendirme sistemi gibi donanımsal ve güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler yazılımsal önlemler alınır.

6.6.1.6 Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenir, bu risklere uygun teknik tedbirlerin alınması sağlanır ve alınan tedbirlere yönelik teknik kontroller yapılır.

"Bu dokümanın güncelliği, elektronik ortamda EYS Yazılımından takip edilmelidir. Basılı kopyalar "Kontrolsüz Kopyadır."

6.6.1.7 PTT AŞ içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılır.

6.6.1.8 Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulur.

6.6.1.9 Silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz hale getirilmesi için gerekli tedbirler alınır.

6.6.1.10 Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenir ve bilgi sistemleri güncel halde tutulur.

6.6.1.11 Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılır.

6.6.1.12 Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılır.

6.6.1.13 Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılır.

6.6.1.14 PTT AŞ internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak şifrelenir.

6.6.1.15 PTT AŞ tarafından, PTT AŞ personeline tahsis edilen taşınabilir disk (USB bellekler ve harici diskler) PTT AŞ işleri haricinde kullanılamaz ve PTT AŞ dışına çıkarılmaz. Taşınabilir diskler kriptolu olarak verilir. Organizasyon dışına çıkarılacak taşınabilir disklerin kayıtları tutulur ve kaydı alınan yetkili çalışan tarafından kullanılır.

6.6.1.16 Taşınabilir diskler içinde PTT AŞ' ye ait kritik veya gizli bilgiler saklanmaz. Eğer kritik veya gizli bilgi taşınması gerekiyorsa taşınma işleminde sonra bu bilgiler tekrar erişilemeyecek şekilde diskten silinir.

6.6.1.17 Üçüncü taraf (tedarikçi) sözleşmelerinde, belirtilen hizmetlerin tanımının, güvenlik seviyesinin ve denetiminin gerçekleştirilmesini ve sürdürülmesini güvence altına almak için "Üçüncü Taraf Bilgi Koruma Taahhütnamesi" imzalattırılır.

6.6.1.18 Kullanıcıların sadece kullanma yetkisine sahip oldukları network (ağ) servislerine erişebilmesi sağlanır.

6.6.2 İdari Tedbirler

6.6.2.1 Tüm personele Kanun ve ikincil mevzuata, Kurul kararlarına ve diğer düzenlemelere uygun bir şekilde kişisel verilerin işlenmesinin sağlanması amacıyla periyodik olarak eğitimler verilir.

6.6.2.2 PTT AŞ tarafından yürütülen faaliyetlere ilişkin personele gizlilik taahhütnameleri imzalatılır.

6.6.2.3 Kişisel veri işlemeye başlamadan önce PTT AŞ tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilir.

6.6.2.4 Kişisel veri işleme envanteri hazırlanır.

6.6.2.5 Alıcı gruplarıyla akdedilen sözleşmelere gizlilik ve kişisel verilerin korunmasına ilişkin maddeler eklenir.

6.6.2.6 İlgili kişinin kişisel verilerini imhaya yönelik talebinin uygun bulunması durumunda alıcı gruplarına aktarılan kişisel verilerin alıcı grupları tarafından da imha edilmesi sağlanır.

6.6.2.7 Fiziki kayıt ortamlarında saklanan kişisel veriler için Ayıklama ve İmha Komisyonu bulunur.

6.6.2.8 Arşiv sorumluları tarafından arşivlere yetkisiz girişlerin engellenmesi ve kişisel verilerin saklandığı fiziksel ortamların güvenliğinin sağlanması için (elektrik kaçağı, yangın, su baskını, hırsızlık vb.) yeterli güvenlik önlemleri alınır.

6.6.2.9 Bilgi güvenliği, özel hayatın gizliliği ve kişisel verilerin korunması alanındaki gelişmeler takip edilir.

"Bu dokümanın güncelliği, elektronik ortamda EYS Yazılımından takip edilmelidir. Basılı kopyalar "Kontrolsüz Kopyadır."

6.6.2.10 PTT AŞ internet sitesinde "Gizlilik" sekmesi içerisinde kişisel verilerin korunmasına ilişkin olarak; aydınlatma metinleri, ilgili kişi başvuru formu gibi dokümanlara yer verilir.

6.7 Özel Nitelikli Kişisel Verilerle İlgili Tedbirler

6.7.1 Verilere erişim yetkisine sahip kullanıcıların, yetki kapsamları ve süreleri belirlenir.

6.7.2 Periyodik olarak yetki kontrolleri gerçekleştirilir.

6.7.3 Görev değişikliği olan ya da işten ayrılan personelin bu alandaki yetkileri kaldırılır.

6.7.4 Veriler kriptografik yöntemler kullanılarak muhafaza edilir.

6.7.5 Kriptografik anahtarlar güvenli ve farklı ortamlarda tutulur.

6.7.6 Veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtları güvenli olarak loglanır.

6.7.7 Verilerin bulunduğu ortamlara ait güvenlik güncellemelerinin sürekli takip edilmesi, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması sağlanır.

6.7.8 Verilere bir yazılım aracılığı ile erişilmesi halinde, bu yazılıma ait kullanıcı yetkilendirmelerinin yapılması, bu yazılımların güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması sağlanır.

6.7.9 Verilere uzaktan erişim halinde en az iki kademeli kimlik doğrulama sistemi sağlanır.

6.7.10 Verilerin e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle aktarılır.

6.7.11 Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenir ve kriptografik anahtar farklı ortamda tutulur.

6.7.12 Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında IPSec VPN kurularak veya kriptolu yöntemlerle veri aktarımı gerçekleştirilir.

7. ONAY

Bu prosedür Yönetim Kurulu tarafından onaylanır.

8. YÜRÜRLÜK

Bu prosedür yayımlandığı tarihte yürürlüğe girer.

9. YÜRÜTME

Bu prosedürü Genel Müdür yürütür.

10. REFERANS DOKÜMANLAR

BTD.PK01-Bilgi Transferi Politikası
BTD.PK03-Bilgi Güvenliği Yedekleme Politikası
BTD.PK05-Şifre Yönetimi Politikası
BTD.PK07-Erişim Kontrol Politikası
BTD.PR02-Haberleşme Güvenliği Prosedürü
BTD.TL08-Erişim Yönetimi Talimatı
DHU.PL02-Saklama Süreli Standart Dosya Planı
EYS.FR22-Üçüncü Taraf Bilgi Koruma Taahhütnamesi
EYS.TL06-Güvenli Alanların Fiziksel ve Çevresel Güvenliği Talimatı
KHK.002-399 Sayılı KHK

"Bu dokümanın güncelliği, elektronik ortamda EYS Yazılımından takip edilmelidir. Basılı kopyalar "Kontrolsüz Kopyadır."

KN.003-5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
KN.005-5070 sayılı Elektronik İmza Kanunu
KN.008-6698 sayılı Kişisel Verilerin Korunması Kanunu
KN.009-5809 sayılı Elektronik Haberleşme Kanunu
KN.010-657 sayılı Devlet Memurları Kanunu
KN.012-6475 sayılı Posta Hizmetleri Kanunu
KN.015-5434 sayılı Türkiye Cumhuriyeti Emekli Sandığı Kanunu
KN.020-4857 sayılı İş Kanunu
KN.022-6331 sayılı İş Sağlığı ve Güvenliği Kanunu
KN.035-6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun
KN.036-6102 sayılı Türk Ticaret Kanunu
KN.037-6098 sayılı Türk Borçlar Kanunu
KN.038-2004 sayılı İcra ve İflas Kanunu
KN.042-7201 sayılı Tebligat Kanunu
KN.044-406 sayılı Telgraf ve Telefon Kanunu
KN.045-5464 sayılı Banka Kartları ve Kredi Kartları Kanunu
KN.046-5411 sayılı Bankacılık Kanunu
KN.048-4982 sayılı Bilgi Edinme Kanunu
KN.049-3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun
RYB.PR02-Kişisel Verilerin Korunması Prosedürü
RYB.PR03-Kişisel Veri İşleme Envanteri Prosedürü
RYB.PR04-Veri Sahibi Başvuru Yönetimi Prosedürü
RYB.PR05-Kişisel Veri Güvenliği Denetim Prosedürü
RYB.PR06-Kişisel Veri Güvenliğine İlişkin İdari ve Teknik Tedbirler Prosedürü
RYB.TB01-Kişisel Verilerin Saklanmasını Gerektiren Hukuki Sebepler Tablosu
YNT.036-Elektronik Tebligat Yönetmeliği
YNT.037-Kayıtlı Elektronik Posta Sistemine İlişkin Usul ve Esaslar Hakkında Yönetmelik
YNT.042-Devlet Arşiv Hizmetleri Hakkında Yönetmelik
YNT.047-Bilgi Teknolojileri Ve İletişim Kurumu Posta Sektöründe İdari Yaptırımlar Yönetmeliği
YNT.067-Posta Hizmetlerinin Sunulmasına İlişkin Yönetmelik
YNT.068-Bilgi Teknolojileri ve İletişim Kurumu Posta Sektöründe İdari Yaptırımlar Yönetmeliği
YNT.078-Evrensel Posta Hizmetleri Yönetmeliği

11. REVİZYON BİLGİLERİ

Revizyon No	Revizyon Tarihi	Revizyon Nedeni
0	**28.07.2025**	**Yeni Doküman**

"Bu dokümanın güncelliği, elektronik ortamda EYS Yazılımından takip edilmelidir. Basılı kopyalar "Kontrolsüz Kopyadır."

"Bu dokümanın güncelliği, elektronik ortamda EYS Yazılımından takip edilmelidir. Basılı kopyalar "Kontrolsüz Kopyadır."