

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Doküman ismi:

TESAN İLETİŞİM A.Ş. Kişisel Veri Saklama ve İmha Politikası

Hedef Kitle:

TESAN İLETİŞİM A.Ş. tarafından kişisel verileri işlenen gerçek kişiler

Onaylayan:

TESAN İLETİŞİM A.Ş. Yönetim Kurulu tarafından onaylanmıştır.

İşbu belge TESAN İLETİŞİM A.Ş.'nin yazılı izni olmaksızın çoğaltılıp dağıtılamaz.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

İÇİNDEKİLER

1. AMAÇ, KAPSAM
2. TANIMLAR
3. SORUMLULUK VE GÖREV DAĞILIMLARI
4. KAYIT ORTAMLARI
5. SAKLAMAYA İLİŞKİN AÇIKLAMALAR
- 5.1. SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER
- 5.2. SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI
6. İMHAYI GEREKTİREN SEBEPLER
7. ALINAN TEKNİK VE İDARİ TEDBİRLER
8. İMHA TEKNİKLERİ
- 8.1. KİŞİSEL VERİLERİN SİLİNMESİ
- 8.2. KİŞİSEL VERİLERİN YOK EDİLMESİ
- 8.3. KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ
9. SAKLAMA VE İMHA SÜRELERİ
10. PERİYODİK İMHA SÜRESİ
11. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI
12. POLİTİKA'NIN GÜNCELLEME PERİYODU
13. POLİTİKA'NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

HAZIRLAYAN	KONTROL	ONAY
Firma Avukatı	Kalite Yöneticisi	Yönetim Kurulu

1.AMAÇ VE KAPSAM

07.04.2016 tarihinde 6698 sayılı "Kişisel Verilerin Korunması Kanunu" (bundan böyle kısaca "Kanun" olarak anılacaktır) yayınlanarak yürürlüğe girmiştir. Söz konusu kanun kapsamında Şirketimiz Tesan İletişim A.Ş., (bundan böyle kısaca "TESAN" olarak anılacaktır) "Veri Sorumlusu" sıfatına sahip olup, bu sıfatın gerektirdiği yükümlülükleri yerine getirmek için gerekli uyum çalışmalarını gerçekleştirmektedir. İşbu Politika'nın amacı, TESAN tarafından gerçekleştirilmekte olan kişisel verilere özgü saklama ve imha faaliyetlerine ilişkin işlemler hususunda usul ve esasları belirlemektir.

İş ortaklarımızın/potansiyel iş ortaklarımızın, tedarikçilerimizin/potansiyel tedarikçilerimizin, bayilerimizin/potansiyel bayilerimizin, müşterilerimizin (tüketiciler de dahil) /potansiyel müşterilerimizin, personel/aday personelin, bursiyerler /aday bursiyerlerin ve ziyaretçilerin kişisel verilerinin ve bu verilerin işlendiği tüm kayıt ortamlarına ilişkin saklama ve imha faaliyetleri işbu Politika'daki esaslara paralel olarak TESAN tarafından yönetilmektedir.

2. TANIMLAR

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

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 mahkumiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verilerdir.

Açık Rıza: Veri öznesinin belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıkladığı rızadır.

Anonim Hale Getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesidir.

Anonim Hale Getirilmiş Veri: Veri öznesi ile hiçbir şekilde ilişkisinin kurulması mümkün olmayan veridir.

Kişisel Veri İşleme: Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.

Veri Öznesi: Kişisel verileri işlenen gerçek kişi.

Veri Sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.

Veri İşleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Kurul: Kişisel Verileri Koruma Kurulu.

Kurum: Kişisel Verileri Koruma Kurumu.

Kanun: 6698 sayılı Kişisel Verilerin Korunması Kanunu.

Yönetmelik: 28.10.2017 tarihli Resmi Gazete’de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

KVK Düzenlemeleri: Kanun ile Kişisel Verilerin Korunmasına yönelik ilgili diğer mevzuat, yönetmelikler, düzenleyici ve denetleyici otoriteler, mahkemeler ve diğer resmi makamlar tarafından verilen bağlayıcı kararlar, ilke kararları, hükümler, talimatlar ile verilerin korunmasına yönelik her türlü mevzuat.

İş Ortağı: TESAN’ın ticari faaliyetlerini yürütürken ürün ve hizmetlerin satışı, tanıtımı ve pazarlaması, satış sonrası desteği, ortak müşteri bağlılığı programlarının yürütülmesi gibi amaçlarla iş ortaklığı kurduğu/kurmak istediği gerçek/tüzel kişi.

Tedarikçi: TESAN’ın ticari faaliyetlerini yürütürken TESAN’ın emir ve talimatlarına uygun olarak hizmet sunan/sunmak isteyen gerçek/tüzel kişi.

Müşteri: TESAN ile herhangi bir sözleşme ilişkisi olup olmadığına bakılmaksızın TESAN’ın sunmuş olduğu ürün ve hizmetleri kullanmış olan/kullanan/satın alan gerçek/tüzel kişidir. TESAN’dan ürün satın almak isteyen/alan gerçek kişi tüketiciler de bu kapsama dahildir.

Potansiyel Müşteri: TESAN ile herhangi bir sözleşme ilişkisi olup olmadığına bakılmaksızın TESAN’ın sunmuş olduğu ürün ve hizmetleri kullanmak/satın almak isteyen gerçek/tüzel kişi.

Bayi: TESAN ile herhangi bir sözleşme ilişkisi olup olmadığına bakılmaksızın TESAN’ın ürünlerini satarak bayilik ilişkisi içine girdiği/girmek istediği gerçek/tüzel kişi.

Personel: TESAN ile iş akdi sözleşmesi imzalayarak daha önce çalışmış olan ya da halen daha çalışmaya devam eden gerçek kişi ve stajyer.

Personel Adayı: TESAN’a herhangi bir yolla iş başvurusunda bulunmuş ya da özgeçmiş ve ilgili bilgilerini TESAN’ın incelemesine açmış olan gerçek kişi ve stajyer.

Ziyaretçi: TESAN’n sahip olduğu fiziksel yerleşkelere çeşitli amaçlarla giren gerçek kişi.

Bursiyer: TESAN’dan burs almaya hak kazanan gerçek kişi.

Bursiyer Adayı: TESAN’dan burs almak için başvuran gerçek kişi.

Alıcı Grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek ve/veya tüzel kişi kategorisi.

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

Elektronik Olmayan Ortam: Elektronik ortamların dışında kalan tüm yazılı, basılı, görsel vs. diğer ortamlar.

EBYS: Elektronik Belge Yönetim Sistemi

Hizmet Sağlayıcı: TESAN ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek ve/veya tüzel kişi.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

İlgili

Kullanıcı: Verilerin teknik olarak depolanması, koruması ve yedeklenmesinden sorumlu olan kişi yada birim hariç olmak üzere veri sorumlusu organizasyonu içerisinde veya veri sorumlusundan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişiler.

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

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

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 ortam.

Kişisel Verileri İşleme Envanteri: İş sürecine bağlı olarak veri sorumlusunun gerçekleştirmekte olduğu veri işleme faaliyetini; kişisel veri işleme amaçları ve hukuki sebepleri, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve amaçlar için gerekli olan azami muhafaza edilme süresi, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırılan envanter.

Politika: Kişisel Verileri Saklama ve İmha Politikası.

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

Veri Sorumluları Sicil Bilgi Sistemi/VERBİS: Veri sorumlularının sicile başvuruda ve sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilşim sistemi.

3. SORUMLULUK VE GÖREV DAĞILIMLARI

TESAN'ın tüm çalışanları, sorumlu birimlerce Politika kapsamına alınmakta ve alınacak olan tüm teknik ve idari tedbirlerin gereği gibi uygulanması doğrultusunda destek verir, talimatlar doğrultusunda hareket eder.

Kişisel verilerin saklama ve imha süreçlerinde görevli olanların ünvanları ve görev tanımları aşağıda yer almaktadır:

- Yönetim Kurulu Başkanı (Birim: Yönetim Kurulu) Politikaların onaylanması, çalışanların politikalara uygun hareket etmesinden sorumludur.
- Bilgi İşlem Yöneticisi, İnsan Kaynakları Yöneticisi, Avukat (Birim: Diğer Birimler) Politikaların hazırlanması, güncellenmesi ve görevlerine uygun olarak Politika'nın yürütülmesinden sorumludur.

4. KAYIT ORTAMLARI

Kişisel veriler, TESAN tarafından aşağıda belirtilen ortamlarda hukuka uygun olarak ve güvenli bir şekilde saklanmaktadır.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

ELEKTRONİK ORTAMLAR	ELEKTRONİK OLMAYAN ORTAMLAR
<ul style="list-style-type: none">Yazılımlar (ofis yazılımları, portal, ERP sistemi)Kişisel bilgisayarlar (Masaüstü, dizüstü)Mobil cihazlar (telefon, tablet v.b.)Bilgi Güvenliği Cihazları (güvenlik duvarı, antivirüs programları, saldırı tespit ve engelleme, yedekleme dosyaları, günlük kayıt dosyası vb.)Optik diskler (DVD, CD vb.)Çıkartılabilir bellekler (USB, Hafıza Kartı vb.)Fotokopi makinesi, faks, yazıcı, tarayıcıVeri depolama sistemleri, sunucular (yedekleme, elektronik posta, veritabanı, web, dosya paylaşımı vb.)	<ul style="list-style-type: none">KağıtManuel veri kayıt sistemleriYazılı, basılı ve görsel ortamlar

5. SAKLAMAYA İLİŞKİN AÇIKLAMALAR

TESAN faaliyetleri çerçevesinde kişisel verileri, ilgili mevzuatta öngörülen veya işleme amaçlarına uygun süre kadar saklamaktadır.

5.1. SAKLAMAYI GEREKTİREN HUKUKİ SEBEPLER

TESAN işbu aşağıda sayılan kanunlar çerçevesinde öngörülen saklama süreleri kadar kişisel verileri saklamaktadır.

* 2709 Sayılı Türkiye Cumhuriyeti Anayasası

*6102 Sayılı Türk Ticaret Kanunu

*6100 Sayılı Hukuk Muhakemeleri Kanunu

*6098 Sayılı Türk Borçlar Kanunu

*4734 Sayılı Kamu İhale Kanunu

*5809 Sayılı Elektronik Haberleşme Kanunu

*5237 Sayılı Türk Ceza Kanunu

*5271 Sayılı Ceza Muhakemesi Kanunu

*4857 Sayılı İş Kanunu

*5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu

*6331 Sayılı İş Sağlığı ve Güvenliği Kanunu

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

*5464 Sayılı Banka ve Kredi Kartları Kanunu

*5846 Sayılı Fikir ve Sanat Eserleri Kanunu

* 7201 Sayılı Tebligat Kanunu

*2813 Sayılı Bilgi Teknolojileri ve İletişim Kurumu Kanunu

* 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

*213 Sayılı Vergi Usul Kanunu

*6493 Sayılı Ödeme Hizmetleri ve Elektronik Para Hakkında Kanun

*6563 Sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun

*6698 Sayılı Kişisel Verilerin Korunması Kanunu

*5070 Sayılı Elektronik İmza Kanunu

*5809 Sayılı Elektronik Haberleşme Kanunu

* Bu kanunlar uyarınca yürürlükte olan yönetmelikler, tebliğler, kararlar vs. diğer tüm ikincil düzenlemeler

5.2. SAKLAMAYI GEREKTİREN İŞLEME AMAÇLARI

TESAN, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri genel olarak aşağıdaki amaçlar doğrultusunda saklamaktadır. Kategori bazında söz konusu amaçlar değişmektedir.

- Kimlik doğrulama ve kayıt oluşturulması amacıyla,
- Siparişlerin işleme konulması ve hesabın yönetilmesi, ticari faaliyetlerin yerine getirilebilmesi ve sürekliliğinin sağlanabilmesi amacıyla,
- TESAN'ın kurumsal iletişiminin yada TESAN ile iş ilişkisinde bulunan 3. Kişilerle iletişimin sağlanması amacıyla,
- Alınan hizmet süreçleri ile alakalı bilgilendirme amacıyla,
- Acil durum yönetimi süreçlerinin yürütülmesi amacıyla,
- Siparişlerin ve kargoların teslimi/iadesi/nakliyesi amacıyla,
- Siparişler ile ilgili şikayetlerin çözülmesi amacıyla,
- Teknik servis hizmetinin verilebilmesi amacıyla,
- Önceden onay verilmesi kaydı ile yeni ürünler, kampanyalar ve promosyonlar hakkında bilgi vermek amacıyla elektronik ileti gönderilmesi amacıyla,
- İşlemlerle ilgili istatistiklerin yapılabilmesi ve bağlantılı listelerin oluşturulması, ticari istatistik ve analizlerin bir araya getirilmesi amacıyla,
- Ürünlerin, hizmetlerin ve kişisel seçim olanaklarının araştırılması ve geliştirilmesi amacıyla,

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

- Tedarik zinciri yönetimi süreçlerinin yürütülmesi amacıyla,
- Yazılım, kurumsal kaynak planlaması, raporlama, pazarlama vs. gibi işlevlerin yerine getirilmesi amacıyla,
- Risk limitlerinin belirlenmesi ve teminatlandırma çalışmalarının yapılması amacıyla,
- Promosyonlar ve kampanyalardan faydalandırılması amacıyla,
- İşyerinde güvenlik uygulamaları nedeniyle,
- Kalite, bilgi güvenliği ve gizlilik politikalarının ve standartlarının sağlıklı olarak temini ve denetimi amacıyla,
- Üst yönetime yapılacak raporlama ve analizlerin hazırlanması amacıyla,
- Kanun ve yönetmelikler ile belirlenmiş gerekliliklerin ifa edilmesi amacıyla (vergi mevzuatı, tüketicilerin korunmasına yönelik mevzuat, borçlar hukuku mevzuatı, ticaret hukuku mevzuatı, gümrük mevzuatı, elektronik iletişim ile ilgili mevzuat vs. ilgili tüm mevzuatlar),
- e-fatura, e-arşiv ve e-irsaliye ile ilgili yükümlülüklerin yerine getirilmesi amacıyla,
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde kamu kurum ve kuruluşlarının taleplerinin yerine getirilmesi amacıyla,
- KVKK'da belirtilmiş yasal yükümlülüklerin yerine getirilmesi amacıyla,
- Aranılan pozisyona uygun olup olunmadığının tespiti amacıyla, uygun olmadığına karar verildiği takdirde benzer pozisyonlarda değerlendirmek amacıyla,
- Personelin istihdamı ile ilgili olarak yasal yükümlülüklerin yerine getirilmesi amacıyla,
- Personele maaş hesabı açılması, gerektiği durumlarda kiralık araç verilmesi, telefon verilmesi, telefon hattı verilmesi, yemek kartı verilmesi, otomatik bireysel emeklilik işlemlerinin yerine getirilmesi gibi personele sağlanan yan haklar ve menfaat süreçlerinin yürütülmesi amacıyla,
- Yabancı personel çalışma ve oturma izin işlemleri amacıyla,
- Çeşitli insan kaynakları uygulamaları amacıyla,
- Acil tıbbi müdahaleler amacıyla,
- Hastalık izinlerinin takibi ve izlenmesi veya personelin görevini yerine getirebilmesi için gerekli sağlık koşullarının takibi amacıyla,
- Personelin maaşına konulan maaş hacizlerinin takibi amacıyla,
- Şirket seyahatlerinin organize edilmesi amacıyla,
- Acil durumların varlığı halinde personelin kendi rızası ile verdiği kişiler ile iletişime geçilmesi amacıyla,
- Personel masraflarının hesaplanması amacıyla,

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

- İşe giriş ve çıkışların tespiti ve kontrolü amacıyla,
- Çalışan memnuniyeti ve bağlılığı süreçlerinin yönetilmesi amacıyla,
- Eğitim faaliyetlerinin yürütülmesi amacıyla,
- Yetenek ve kariyer gelişimi faaliyetlerinin yürütülmesi amacıyla,
- Erişim yetkilerinin yürütülmesi amacıyla,
- Firma/ürün/hizmetlere bağlılık süreçlerinin yürütülmesi amacıyla,
- Performans değerlendirmesi yapmak ve ücret politikaları belirlemek amacıyla,
- İşyerinde gizlilik ve güvenlik uygulamaları nedeniyle kamera görüntülerinin kaydedilmesi,
- Burs verilmesine ilişkin şartlara uygun olup olmadığının tespiti amacıyla,
- Bursiyer ve bursiyerin kendi rızası ile bilgilerini verdiği kişiler ile iletişime geçilmesi amacıyla,
- İnternet hizmeti verilebilmesi amacıyla,
- Giriş ve çıkışların tespiti ve kontrolü amacıyla,
- Ziyaretçi kayıtlarının oluşturulması ve takibi amacıyla,

Kişisel veri öznesinin açık rızasını vermemesi durumunda yukarıdaki amaca giren ilgili iş birimlerinin tüm kişisel veri işleme faaliyetlerinin yapılamaması değil; ilk paragrafta belirtilen veri öznesinin veri işlemeye yönelik açık rızasına gerek olmayan aynı amaç kapsamı içindeki kişisel veri işleme faaliyetlerinin dışında kalan ve bu amaca yönelmiş ilgili iş birimlerinin kişisel veri işleme faaliyetlerinin yapılamayacağı anlamı çıkmalıdır.

6. İMHAYI GEREKTİREN SEBEPLER

TESAN, aşağıda sayılan sebeplerin varlığı durumunda kişisel verileri siler, yok eder yada anonim hale getirir. Söz konusu sebepler;

- İlgili mevzuat hükümlerinin değiştirilmesi ya da ortadan kalkması,
- İşlenmeyi ya da saklanmayı gerektiren amacın ortadan kalkması,
- Kişisel veri işleminin sadece açık rıza şartına bağlı olduğu hallerde, ilgili kişinin açık rızasını geri alması,
- Kanununun 11. Maddesi gereği ilgili kişinin hakları çerçevesinde yaptığı başvurunun kabul edilmesi,
- TESAN'ın ilgili kişinin talebi ile kendisine yapılan başvuruyu reddetmesi, ilgili kişi tarafından cevabın yetersiz bulunması veya süresi içinde cevap vermemesi hallerinde, Kurul'a şikayette bulunması ve Kurul'un bu talebe uygun olarak karar vermesi,
- Kişisel verinin saklanmasını gerektiren azami sürenin geçmiş olması ve daha uzun süre saklamayı gerektiren bir şartın olmaması

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

7.ALINAN TEKNİK VE İDARİ TEDBİRLER

TESAN, kişisel verilerin ve özel nitelikli kişisel verilerin güvenli bir şekilde muhafaza edilmesi, hukuka aykırı olarak işlenmesi, yetkisiz kişilerce erişiminin önlenmesi ve hukuka uygun olarak imha edilmesi için kanunun ve Kurul'un belirlediği yeterli önlemler çerçevesinde teknik ve idari tedbirler almaktadır. Alınan teknik ve idari tedbirler;

- TESAN tarafından tüm iş süreçleri irdelenerek veri envanteri çıkarılmıştır. TESAN'ın yürütmekte olduğu tüm faaliyetler detaylı olarak analiz edilerek, bu analiz neticesinde kişisel veri işleme faaliyetleri ortaya konulmaktadır.
- VERBİS sistemine süresi içinde kayıt yaptırılacaktır.
- TESAN, veri kategorilerine göre aydınlatma metinlerini hazırlamış ve veri öznelerine söz konusu aydınlatma metinlerini bildirmiştir. Ayrıca, TESAN sahibi olduğu internet sitelerine de aydınlatma metinlerini herkesin erişimine açık şekilde sunmuştur.
- TESAN, kanunen gerekmesi halinde veri öznelerinden açık rıza almaktadır.
- Kişisel veri ve bilgi güvenliğine ilişkin politikalar ve prosedürler belirlenmekte ve gerektiğinde güncellenmektedir.
- Kişisel verilerin mümkün olduğunca azaltılmasına yönelik çalışmalar yapılmaktadır.
- TESAN tarafından kişisel verilerin hukuka uygun olarak aktarıldığı kişiler ile sözleşmeler yapılmakta ve sözleşmelere Kanun'a uygun olarak veri işleme faaliyeti yapılacağına, güvenlik tedbirleri alacaklarına dair hükümler konulmaktadır.
- TESAN sahibi olduğu internet sitelerinde SSL sistemi uygulanmaktadır.
- TESAN' ait tüm bilgisayarlarda anti virüs sistemleri kullanılmaktadır.
- Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
- Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
- Veri kaybı önleme yazılımları kullanılmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakım kapsamındaki güvenlik önlemleri alınmaktadır.
- Bilişim sistemlerinin sürekliliğini etkileyecek riskler izlenmekte ve risk tespit edildiği zaman gerekli önlemler alınmaktadır.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi ile ilgili kurallar belirlenmekte ve bu kurallara uygun hareket edilmektedir.
- TESAN'ın sahibi olduğu bilişim sistemleri teçhizatları, yazılımları ve verilerinin fiziksel güvenliği için gerekli tüm önlemler alınmaktadır.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

- Sistem odasına sadece yetkili personelin girişini sağlayan erişim kontrol sistemi bulunmaktadır.
- TESAN'ın ve kişilerin güvenliği için 7/24 çalışan kamera sistemi bulunmaktadır.
- Teknolojideki gelişmelere uygun teknik önlemler alınmakta, alınan önlemler periyodik olarak güncellenmektedir.
- TESAN bünyesinde gerçekleştirilen kişisel veri işleme faaliyetleri mevcut olan ve kurulan teknik sistemlerle denetlenmektedir.
- İş yeri güvenliği ile ilgili alınması gereken tüm önlemler (yangın söndürme vb.) alınmıştır.
- Virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar kurulmakta ve gerektiğinde güncellenmekte ya da yenilenmektedir.
- Kişisel verilerin kaybolmasını yahut zarar görmesini engellemek üzere yedekleme programları kullanılmakta ve yeterli düzeyde güvenlik önlemleri alınmaktadır.
- TESAN, Bilgi güvenliği standardı olan ISO 27001 belgesini almış ve gerekliliklerine uygun hareket etmektedir.
- Kişisel verilerin işlendiği elektronik ortamlarda loglama sistemleri kullanılmaktadır. Erişim logları düzenli olarak tutulmaktadır. Log kayıtları kullanıcı müdahalesi olmayacak şekilde tutulmaktadır.
- Kişisel verilerin saklandığı ve işlendiği ortamlarda güçlü parolalar kullanılmaktadır.
- Sızma testi yaptırılmaktadır.
- Kişisel verilerin güvenli ortamlarda saklanması ve hukuka aykırı amaçlarla yok edilmesini, kaybolmasını veya değiştirilmesini önlemek için teknolojik imkanlar ve uygulama maliyetine göre gerekli tedbirler alınmaktadır.
- Şirket personeli bilgi güvenliği ve kişisel verilerin korunması konusunda bilgilendirilmekte ve eğitilmektedir.
- TESAN ile personel arasında yapılan sözleşmelere gizlilik ve gizlilik ihlali ile ilgili maddeler konulmaktadır.
- Şirket personeli, kişisel verilerin güvenliğine ve gizliliğine ilişkin yükümlülüklerinin, iş ilişkisinin sona ermesinden sonra da devam edeceği konusunda bilgilendirilmiş ve Şirket personelinin bu kurallara uymaları yönünde taahhüt alınmıştır.
- Personel'in zimmetinde olan tüm dolapların anahtarı bulunmakta olup, gerekmediği durumlarda dolaplar sürekli kitlidir.
- Kendisine şirket cihazı tahsis edilen her kişi, kendi kullanımına tahsis edilen cihazların güvenliğinden sorumlu olduğunu bilmekte ve zimmet formu imzalamaktadır.
- Her şirket personeli kendi sorumluluk alanında yer alan fiziki dosyaların güvenliğinden sorumlu olduğunu bilmektedir.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

- Özel nitelikli kişisel verilerin işlendiği ve muhafaza edildiği fiziksel ortamlarda yeterli güvenlik önlemleri alınmakta ve fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecek ise mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- Özel nitelikli kişisel verilere ilişkin prosedürler belirlenmiştir.
- Özel nitelikli kişisel veriler için güvenli şifreleme kullanılmaktadır.
- Taşınabilir bellek ile aktarılan özel nitelikli kişisel veriler şifrelenerek aktarılmaktadır.
- İş birim bazlı kişisel verilere erişim ve yetkilendirme süreçleri uygulanmaktadır.
- TESAN, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılmaz olması için gerekli tedbirleri almaktadır.
- Görev değişikliği olan ya da işten ayrılan personelin giriş yetkileri ve erişimleri kaldırılmaktadır.
- TESAN adına veri işleyen hizmet sağlayıcılar ile sözleşmeler yapılmakta olup veri güvenliği konusunda farkındalık sağlanmaktadır.
- TESAN, kanunun ve Kurul'un kararları doğrultusunda gerekli ve şirkete uygun olan teknik ve idari tedbirleri almaktadır.

8. İMHA TEKNİKLERİ

TESAN'ın bünyesinde işlediği kişisel verilerin imhasını gerektirecek bir durum söz konusu olduğunda TESAN ilgili mevzuat hükümlerine uygun olarak ve aşağıda yer alan tekniklerle kişisel verileri imha eder. Kişisel verilerin imhasına ilişkin süreç aşağıda açıklanmaktadır;

- * Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi
- * Her bir kişisel veri için ilgili kullanıcıların tespit edilmesi
- * İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi
- * İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerin kapatılması ve ortadan kaldırılması

8.1. KİŞİSEL VERİLERİN SİLİNMESİ

Sunucularda yer alan kişisel veriler sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silinir.

Bulut sisteminde yer alan kişisel veriler silme komutu verilerek silinir.

Elektronik ortamda yer alan kişisel veriler veri tabanı yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Kağıt ortamında yer alan kişisel veriler ilgili birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılmaz hale getirilir. Ayrıca, üzeri okunmayacak şekilde çizilerek, boyanarak ve/veya silinerek karartma işlemi uygulanır.

Taşınabilir medyada yer alan kişisel veriler sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarıyla güvenli ortamda saklanır. Bu ortamlara uygun yazılımlar kullanılarak silinmektedir.

Veri tabanlarında yer alan kişisel veriler bulunduğu ilgili satırın veri tabanı konutu ile (delete vb.) silinmektedir.

8.2. KİŞİSEL VERİLERİN YOK EDİLMESİ

Fiziksel ortamda yer alan kişisel veriler kağıt kırma makinelerinde geri dönülmeyecek şekilde yok edilir.

Optik medya ve manyetik medyada yer alan kişisel veriler yakılarak veya toz haline getirilir. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılarak üzerindeki veriler okunmaz hale getirilebilir.

8.3. KİŞİSEL VERİLERİN ANONİM HALE GETİRİLMESİ

Kişisel veriler anonim hale getirilerek, verilerin geri döndürülmesi ve/veya başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmektedir. Anonim hale getirme işlemi "genelleştirme" yöntemi ile yapılmaktadır. Bu yöntem; ilgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkansız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir.

9. SAKLAMA VE İMHA SÜRELERİ

TESAN, ilgili kanunlarda öngörülmesi durumunda kişisel verileri öngörülen süre boyunca saklamakla yükümlüdür. Kişisel verilerin ne kadar süre boyunca saklanması gerektiğine ilişkin kanunlarda bir süre öngörülmemiş ise, kişisel veriler, TESAN'ın o veriyi işlerken yürütülen faaliyete bağlı olarak TESAN'ın uygulamaları ve ticari yaşamın teamülleri uyarınca işlenmesi gerektiren süre kadar işlenmekte, daha sonra silinmekte, yok edilmekte veya anonim hale getirilmektedir.

Kişisel verilerin saklanma süreleri veri öznesi kategorilerine göre ayrı ayrı belirlenmiş olup, ilgili aydınlatma metinlerinde, veri envanterinde ve politikada açıkça düzenlenmiştir.

Kişisel verilerin işleme amacı sona ermiş; ilgili kanun ve TESAN'ın belirlediği saklama sürelerinin de sonuna gelmişse; kişisel veriler yalnızca olası hukuki uyuşmazlıklarda delil teşkil etmesi veya kişisel veriye bağlı ilgili hakkın ileri sürülebilmesi veya savunmanın tesis edilmesi amacıyla saklanabilmektedir. Buradaki sürelerin tesisinde bahsi geçen hakkın ileri sürülebilmesine yönelik zaman aşımı süreleri ile zaman aşımı sürelerinin geçmesine rağmen daha önce aynı konularda TESAN'a yöneltilen taleplerdeki örnekler esas alınarak saklama süreleri belirlenmektedir. Bu durumda saklanan kişisel verilere herhangi bir başka amaçla erişilmemekte ve ancak ilgili hukuki uyuşmazlıkta kullanılması gerektiği zaman ilgili kişisel verilere erişim sağlanmaktadır.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Burada da bahsi geçen süre sona erdikten sonra kişisel veriler silinmekte, yok edilmekte veya anonim hale getirilmektedir.

Söz konusu saklama süreleri üzerinde gerekmesi halinde TESAN tarafından güncelleme yapılacaktır. TESAN'ın saklama ve imza süreleri aşağıda yer almaktadır:

* Ziyaretçilere ait kişisel veriler 6 (altı) ay boyunca saklanmaktadır. Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde imha edilecektir.

*Bursiyerlere ait kişisel veriler burs ilişkisi sona erdikten itibaren 5 (beş) yıl boyunca saklanmaktadır. Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde imha edilecektir.

*İş ortakları, bayiler ve tedarikçilere ait kişisel veriler ticari ilişki sona erdikten sonra 10 (on) yıl boyunca, potansiyel iş ortakları, bayiler ve tedarikçilere ait kişisel veriler TESAN'a başvuru yaptıktan itibaren 1 (bir) yıl boyunca saklanmaktadır. Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde imha edilecektir.

* Personele ait kişisel veriler iş akdi sona erdikten sonra 10 (on) yıl boyunca, aday personelin kişisel verileri başvuru tarihinden itibaren 1 (bir) yıl boyunca saklanmaktadır. Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde imha edilecektir.

* Müşterilere ait kişisel veriler ticari ilişki sona erdikten sonra 10 (on) yıl boyunca saklanmaktadır. Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde imha edilecektir.

*Log kayıtları 2 (iki) yıl boyunca saklanmaktadır. Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde imha edilecektir.

*Kamera kayıtları 6 (altı) ay boyunca saklanmaktadır. Saklama süresinin bitimini takip eden ilk periyodik imha sürecinde imha edilecektir.

10. PERİYODİK İMHA SÜRESİ

Periyodik imha süresi 6 ay olarak belirlenmiş olup, her yıl Haziran ve Aralık aylarında periyodik imha işlemi gerçekleştirilir.

11. POLİTİKA'NIN YAYINLANMASI VE SAKLANMASI

İşbu Politika TESAN'ın sahibi olduğu internet sitesinde yayımlanır. Basılı kağıt nüshası da yetkili kişinin imzalamasını müteakip hukuk departmanının da muhafaza edilir.

12. POLİTİKA'NIN GÜNCELLEME PERİYODU

İşbu politika TESAN tarafından gerekli görüldüğü takdirde revize edilecek olup, tüm versiyonlar tarih sırası ile www.tesan.com.tr, www.ttec.com.tr ve varsa başkaca internet sitelerinde herkese açık olarak yayımlanır.

13. POLİTİKA'NIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, internet sitesinde yayınlanarak yürürlüğe girecektir. Yürürlükten kaldırılmasına karar verilirse eski nüshanın üzerine iptal kaşesi basılarak, hukuk departmanında 5 (beş) yıl boyunca muhafaza edilir.

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI**14.****REFERANS ve İLGİLİ DOKÜMANLAR****14.1. Referans**

07.04.2016 tarihli 6698 sayılı "Kişisel Verilerin Korunması Kanunu"

28.10.2017 tarihli "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"

30.12.2017 tarihli "Veri Sorumluları Sicili Hakkında Yönetmelik"

10.03.2018 tarihli "Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ"

10.03.2018 tarihli "Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ"

14.2. İlgili Dokümanlar

KVKK PLT-01 Kişisel Verilerin Korunması ve İşlenmesi Politikası

Veri Öznelerine Özel Aydınlatma Metinleri

Veri Öznelerine Özel Açık Rıza Metinleri

15. REVİZYON TAKİBİ

Bu bölümde dokümanın zamanla değişen ihtiyaçlara göre revize edilmesi durumunda bu revizyonlara ilişkin bilgiler yer alır. Revizyon numarası, revizyonun gerekçesi, revize edilen ya da eklenen hususlar, değişikliği isteyen birim ya da kişiler belirtilir.

REVİZYON NO	REVİZYON TARİHİ	REVİZYON GEREKÇESİ VE REVİZYON
00	-	ISO 27001:2013 şartlarını da karşılayan Bilgi Güvenliği Yönetim Sistemi kurma projesi sırasında ilk kez hazırlanmış olan dokümandır.
01	16.12.2019	6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında gözden geçirilip, doküman kodları değiştirilmiştir.