Dnb Analytics

KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

1. GİRİŞ

1.1 Amaç

İşbu Kişisel Veri Saklama ve İmha Politikası, 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve 28 Ekim 2017 tarihli Resmi Gazete'de yayımlanarak 1 Ocak 2018 tarihi itibariyle yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik uyarınca veri sorumlusu sıfatını haiz olan Şirketimiz DNB Analytics Medya Bilişim Pazarlama Danışmanlık Hizmetleri LTD. ŞTİ. Ve şirket bünyesinde faaliyet gösteren iş bu site olan www.dnbanalytics.com tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır. Politika ile kişisel verilerinizin işlendikleri amaç için gerekli olan azami süreyi belirleme esasları ile silme, yok etme ve anonim hale getirme süreçleri hakkında bilgilendirme sağlanması amaçlanmaktadır.

Kişisel verilerin saklanması ve imhasına ilişkin iş ve işlemler, Şirketimiz tarafından bu doğrultuda hazırlanmış olan Politikaya uygun olarak gerçekleştirilir.

1.2 Kapsam

İşbu Politikanın kapsamına Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler dahil olup, Şirket'in sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

2. TANIMLAR

- **Açık Rıza:** Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
- **Alıcı Grubu:** Veri Sorumlusu tarafından kişisel verilerin aktarıldığı gerçek 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 ve diğer otamlar.
- **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 kişiler.

• **İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi. • **Hizmet Sağlayıcı:** Şirketimiz'e belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.

• **Kayıt Ortamı**: Tamamen veya kısmen otomatik olan ya da herhangi bir verikayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamı.

• **KVKK:** 6698 Sayılı Kişisel Verilerin Korunması Kanunu.

• **Kişisel Veri:** Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi. • **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 envanter.

• **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, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem**.**

• **Kişisel Verilerin Anonim Hale Getirilmesi:** Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi işlemi.

• **Kişisel Verilerin Silinmesi:** Kişisel verilerin silinmesi; kişisel verilerin İlgili Kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemi. • **Kişisel Verilerin Yok Edilmesi:** Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi.

• **Kurul:** Kişisel Verileri Koruma Kurulu.

1. **Şirket:** DNB Analytics Medya Bilişim Pazarlama Danışmanlık Hizmetleri LTD. ŞTİ. 2. **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 verileri.

3. **Periyodik İmha:**KVKK'da yer alan kişisel verilerin işlenme 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.
4. **Politika:** İşbu Kişisel Veri Saklama ve İmha Politikası.
5. **Veri İşleyen:** Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi.

6. **Veri Kayıt Sistemi:** Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistem.
7. **Veri Sahibi/İlgili Kişi:** Kişisel verisi işlenen gerçek kişi.
8. **Veri Sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi. 9. **Veri Sorumluları Sicili 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 sistemi. 10. **Yönetmelik:** 28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanan ve 1 Ocak 2018 tarihi itibariyle yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

3. İLKELER

Politika'nın hazırlanmasında, uygulanmasında ve kişisel verilerin işlenmesinde Yönetmelik'in 7. maddesinde yer alan aşağıdaki ilkelere uyulmaktadır.

-KVKK'nın 5. ve 6. maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel veriler veri sorumlusu tarafından resen veya ilgili kişinin talebi üzerine silinir, yok edilir veya anonim hale getirilir.

-Kişisel verilerin silinmesinde KVKK'nın 4. maddesinde sayılan aşağıdaki ilkelere tamamen uyulmaktadır:

a) Hukuk ve dürüstlük kurallarına uygun olma,
b) Doğru ve gerektiğinde güncel olma,
c) Belirli, açık ve meşru amaçlar için işlenme,
d) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

e) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

-KVKK'nın 12. maddesi kapsamında düzenlenen teknik ve idari tedbirlere uyulmaktadır.
-Kurul kararlarına uygun hareket edilmektedir.

-Kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi ile ilgili yapılan tüm işlemler kayıt altına alınır ve söz konusu kayıtlar, diğer hukuki yükümlülükler hariç olmak üzere en az 3 yıl süreyle saklanmaktadır.

-Veri sorumlusu, kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanı seçmektedir. İlgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçecektir.

4. KAYIT ORTAMLARI

Siz veri sahiplerine ait kişisel veriler, şirketimiz tarafından aşağıdaki tabloda listelenen ortamlarda başta KVKK hükümleri olmak üzere diğer ilgili mevzuata uygun olarak güvenli bir şekilde saklanmaktadır.

Elektronik Ortamları : DNB Analytics Medya Bilişim Pazarlama Danışmanlık Hizmetleri LTD.ŞTİ.'ait sunucularda

5. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

5.1. Saklamaya İlişkin Açıklamalar

Şirketimiz tarafından; çalışanlar, çalışan adayları, ziyaretçiler ve hizmet sağlayıcı olarak ilişkide bulunulan üçüncü kişilerin, kurumların veya kuruluşların çalışanlarına ait kişisel veriler KVKK'ya uygun olarak saklanır ve imha edilir.

KVKK m. 3'te kişisel verilerin işlenmesi kavramı tanımlanmış, m. 4'te işlenen kişisel verilerin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen süre kadar muhafaza edilmesi gerektiği belirtilmiş, m. 5'te ise kişisel verilerin işleme şartları sayılmıştır.

Buna göre, Şirketimiz faaliyetleri çerçevesinde kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarımıza uygun süre kadar saklanır.

5.2 Saklamayı Gerektiren Hukuki Sebepler

Şirketimizde faaliyetlerimiz kapsamında işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

• 6698 sayılı Kişisel Verilerin Korunması Kanunu,

• 6502 Sayılı Tüketicinin Korunması Hakkında Kanun

• 6102 sayılı Türk Ticaret Kanunu,
• 6098 sayılı Türk Borçlar Kanunu,

• 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,

• 213 sayılı Vergi Usul Kanunu,

• 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,

• 6361 sayılı İş Sağlığı ve Güvenliği Kanunu,

• 4982 Sayılı Bilgi Edinme Kanunu,

• 3071 sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,

• 4857 sayılı İş Kanunu,

• 5464 Sayılı Banka Kartları ve Kredi Kartları Kanunu

• 6585 Sayılı Perakende Ticaretin Düzenlenmesi Hakkında Kanun

• Abonelik Sözleşmesi Yönetmeliği

• Banka Kartları ve Kredi Kartları Hakkında Yönetmelik

• Kampanyalı Satışlara İlişkin Uygulama Usul ve Esasları Hakkında Yönetmelik

• Mesafeli Sözleşmelere Dair Yönetmelik

• Satış Sonrası Hizmetler Yönetmeliği

• Taksitle Satış Sözleşmeleri Hakkında Yönetmelik

• Tanıtma Ve Kullanma Kılavuzu Yönetmeliği

• Ticari Reklam ve Haksız Ticari Uygulamalar Yönetmeliği

• İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,

• Arşiv Hizmetleri Hakkında Yönetmelik

• Kredi Kartı İşlemlerinde Uygulanacak Azami Faiz Oranları Hakkında Tebliğ • Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri

kadar saklanmaktadır.

5.3 Saklamayı Gerektiren İşleme Amaçları

✓ Potansiyel müşteri/iş ortaklarını değerlendirme

✓ Müşteri ilişkilerinin kurulması ve yönetimi, müşteri/iş ortaklarımızla sözleşme sürecinin yürütülmesi ve sonuçlandırılması (Şirketimizin sunduğu hizmetlerin satış işlemlerinin gerçekleştirilmesi, teklif sunulması, faturalandırma, sözleşme kurulması ve ifa edilmesi, sözleşme sonrası hukuki işlem güvenliğinin sağlanması, hizmet geliştirmek, yeni teknoloji ve uygulamaların değerlendirilmesi ile Şirketimizin ticari ve iş stratejilerinin belirlenmesi ve uygulanması, operasyonların yönetilmesi, finans operasyonları, mali işlerin yönetilmesi, ticari ilişki içerisinde olduğu gerçek/tüzel alternatifler sunabilmek vb.)

✓ Doğrudan Pazarlama Süreçlerinin Yürütülmesi (Memnuniyet anketleri yapılması ya da sosyal medya, online platformlar veya başka mecralar üzerinden yaptığınız görüş, şikayet ve yorumların değerlendirilmesi, dönüş yapılması)

✓ İletişim Ve Destek (Talebiniz Üzerine Hizmetlerimizle ilgili bilgi alma taleplerinin yanıtlanması, iletişim kanallarımız aracılığıyla gelen taleplere ilişkin destek sağlanması, kayıtlarımızın ve veri tabanımızın güncellenmesi)

✓ Yasal Yükümlülüklere Uyma (6698 sayılı Kişisel Verilerin Korunması Kanunu, 6502 Sayılı Tüketicinin Korunması Hakkında Kanun, 6102 Sayılı Türk Ticaret Kanunu, 6098 Sayılı Türk Borçlar Kanunu, 5237 Sayılı Türk Ceza Kanunu başta olmak üzere, ilgili mevzuattan kaynaklanan yasal yükümlülüklerimizin yerine getirilmesi, resmi/özel kurumlar nezdindeki süreçlerin yürütülmesi, kayıt tutma ve bilgilendirme yükümlülükleri, uyum ve denetim, resmi mercilerin denetim ve teftişleri, yasal haklarımızın ve davalarımızı takibi ve sonuçlandırılması, resmi mercilerin talebi üzerine veri ifşası gibi tabi olduğumuz kanun ve düzenlemelere uyum kapsamında gerekli süreçlerin yürütülmesi, düzenleyici ve denetleyici kurumlarla, yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde KVKK'da belirtilmiş yasal yükümlülüklerin yerine getirilmesini sağlamak üzere belirlenmiş gereklilik ve zorunluluklar kapsamında)

✓ Şirket Menfaatlerinin Korunması Ve Güvenliğinin Sağlanması (Şirket çıkarlarının ve menfaatlerinin korunması için gerekli denetim faaliyetlerinin yürütülmesi, Şirketimizle iş ilişkisinde olan kişilerin hukuki ve ticari güvenliğinin temini, sunduğumuz hizmetlerin geliştirilmesi için gerekli çalışmaların yürütülmesi, işyeri

kurallarının uygulanması ve denetlenmesi,sosyal sorumluluk aktivitelerinin planlanması ve icrası, bina içinde meydana gelen tüm olay, kaza, şikayet, kayıp çalıntı vb. durumların raporlanarak gerekli müdahalenin yapılması ve önlem alınması, bakım ve onarım yapılması sırasında oluşabilecektehlikeli durumlar için uyulması gereken kuralların aktarılmasıvb)

✓ Şirket ticari faaliyetlerinin planlanması ve icrası (Şirket'in kısa, orta ve uzun vadede ticari

politikalarının tespit edilmesi, planlanması ve uygulanması, ticari ve iş stratejilerinin belirlenmesi ve uygulanması amacı doğrultusunda; Şirketimiz tarafından yürütülen iletişim, pazar araştırması ve sosyal sorumluluk aktiviteleri, satın alma, gümrük işlemlerinin yürütülmesi, ithalat ihracat operasyonlarında serbest dolaşıma girmiş eşyanın nakliyesinin organizasyonu)

- ✓ Hak Ve Menfaatlerinin Korunması (Şirketimiz aleyhine açılan dava, soruşturma vb. hukuki hak taleplerine karşı savunma)

5.4. İmhayı Gerektiren Sebepler

Kişisel veriler;

• İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi

veya ilgası, • İşlenmesini veya saklanmasını gerektiren amacın ortadan

kalkması,

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

• Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi

ve yok edilmesine ilişkin yaptığı başvurunun Kurum tarafından kabul edilmesi, • Kurumun, ilgili kişi tarafından kişisel verilerinin silinmesi, yok edilmesi veya anonim hale getirilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabı yetersiz bulması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunması ve bu talebin Kurul tarafından uygun bulunması,

• Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olması ve kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması, durumlarında, Kurum tarafından ilgili kişinin talebi üzerine silinir, yok edilir ya da re'sen silinir, yok edilir veya anonim hale getirilir.

6. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerinizin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi, erişilmesinin önlenmesi verilerin hukuka uygun olarak imha edilmesi amacıyla Kanun'un 12.maddesindeki ilkeler çerçevesinde şirket tarafından alınmış tüm idari ve teknik tedbirler aşağıda sayılmıştır.

İdari Tedbirler

Şirket İdari Tedbirler Kapsamında;

- ▪ Saklanan kişisel verilere Şirket içi erişimi iş tanımı gereği erişmesi gerekli personel ile sınırlandırılır. Erişimin sınırlandırılmasında verinin özel nitelikli olup olmadığı ve önem derecesi de dikkate alınır.
- ▪ İşlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi halinde, bu durumu en kısa sürede ilgilisine ve Kurul'a bildirir.
- ▪ Kişisel verilerin paylaşılması ile ilgili olarak, kişisel verilerin paylaşıldığı kişiler ile kişisel

verilerin korunması ve veri güvenliğine ilişkin çerçeve sözleşme imzalar yahut mevcut sözleşmesine eklenen hükümler ile veri güvenliğini sağlar.

▪ Kişisel verilerin işlenmesi hakkında bilgili ve deneyimli personel istihdam eder ve personeline kişisel verilerin korunması mevzuatı ve veri güvenliği kapsamında gerekli eğitimleri verir.

▪ Kendi tüzel kişiliği nezdinde Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar ve yaptırır. Denetimler sonucunda ortaya çıkan gizlilik ve güvenlik zafiyetlerini giderir.

▪ Kişisel verilerin bulunduğu ortama göre yeterli güvenlik önlemlerinin alınmasını sağlar ve bu ortamlara yetkisiz giriş çıkışları engeller.

Teknik Tedbirler

Şirketimiz tarafından, işlediği kişisel verilerle ilgili olarak alınan teknik tedbirler aşağıda sayılmıştır:

• Sızma (Penetrasyon) testleri ile Kurumumuz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır. • Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir. • Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır. • Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.

• Çevresel tehditlere karşı bilişim sistemleri güvenliğinin sağlanması için, donanımsal (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 vb.) ve yazılımsal (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.

• Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.

• Kurum içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır

• Kurum, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.

• Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Kurum tarafından buna uygun bir sistem ve altyapı oluşturulmuştur.

• Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.

• Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır. • Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.

• Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.

• Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.

• Kurum internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.

• Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir. • Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.

• Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması,

• Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamların yeterli güvenlik önlemleri alınmakta, fiziksel güvenliği sağlanarak yetkisiz giriş çıkışlar engellenmektedir.

• Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya sFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı

gerekli önlemler alınmakta ve evrak “gizli” formatta gönderilmektedir.

7. KİŞİSEL VERİLERİN İMHA TEKNİKLERİ

7.1. Kişisel Verilerin Silinmesi

Şirketimiz ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri silebilir. Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirketimizce, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirler alınır.

Kişisel Verilerin Silinmesi Süreci

Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki

gibidir: • Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi.

• Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak 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 yöntemlerinin kapatılması ve ortadan kaldırılması.

Kişisel Verilerin Silinmesi Yöntemleri

Veri Kayıt Ortamı	Açıklama
Sunucularda Yer Alan Kişisel Veriler	Sunucularda yer alan kişisel verilerden saklanmasını gerektirensüre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.
ElektronikOrtamda Yer Alan Kişisel Veriler	Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir. Buna ilişkin örnekler aşağıda yer almaktadır:

• Hizmet Olarak Uygulama Türü Bulut Çözümleri (Office 365 Salesforce, Dropbox gibi:

Bulut sisteminde veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

- Merkezi Sunucuda Yer Alan Ofis Dosyaları: Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının kaldırılması gerekir. Anılan işlem gerçekleştirilirken ilgili kullanıcının ayni zamanda sistem yöneticisi olmadığına dikkat edilmelidir.

7.2. Kişisel Verilerin Yok Edilmesi

Şirketimiz ilgili kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kendi kararına istinaden veya kişisel veri sahibinin talebi üzerine kişisel verileri yok edebilir. Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

Yazılımdan Güvenli Olarak Silme: Tamamen veya kısmen otomatik olan yollarla işlenen ve dijital ortamlarda muhafaza edilen veriler silinirken/yok edilirken; bir daha kurtarılamayacak biçimde verinin ilgili yazılımdan silinmesine ilişkin yöntemler kullanılır.

Kişisel Verilerin Yok Edilmesi Yöntemleri

Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin bulunduğu sistemlerin türüne göre aşağıda yer verilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gereklidir.

Çevresel Sistemler: Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır: İ) Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. ii) Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları, destekleniyorsa <blockerase> komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. iii) Manyetik bant: Verileri esnek bant üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir. iv) Manyetik disk gibi üniteler: Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. Çok güçlü manyetik ortamlara maruz bırakıp de-manyetize ederek ya da yakma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir. v) Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. vi) Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilmesi gerekir. vii) Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak

izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir. viii) Veri kayıt ortamı sabit olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Söz konusu sistemlerin çoğunda silme komutu bulunmakta, ancak yok etme komutu bulunmamaktadır. (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

Bulut Ortamı: Söz konusu sistemlerde yer alan kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle şifrelenmesi ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir. Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir: i) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi, ii) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı servis gibi üçüncü kurumlara gönderilmesi, iii) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir

7.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim haline getirilmesi kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Kişisel verilerin anonim hale getirilmiş olması için kişisel verilerin veri sorumlusu veya üçüncü kişiler tarafından geri döndürülmesi ve/veya verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliğin belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesidir. Anonim hale getirmeye ilişkin yöntemlerde gerekli bilimsel öğretilerden faydanılacaktır. Bu kapsamda değişkenleri çıkartma, kayıtları çıkartma, bölgesel gizleme, genelleştirme, alt ve üst sınır kodlama, global kodlama, örnekleme vb. yöntemler kullanılacaktır.

8. PERSONEL

Şirket'in tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve

farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliği sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Kişisel veri saklama ve imha sürecinde yer alan personelin unvanlarına, birimlerine ve görev tanımlarına işbu Politika'nın EK-1'nde yer alan tablodan ulaşabilirsiniz.

9.SAKLAMA VE İMHA SÜRELERİ

Şirketimiz tarafından faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;
- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde; - Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikası'nda yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde şirketimizin kişisel veriler ile ilgilenen departmanı/birimi tarafından güncellemeler yapılır. Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme ya da anonim hale getirme işlemi kişisel veriler ile ilgilenen departmanı/birimi tarafından yerine getirilir.

Şirketimiz tarafından KVKK ve diğer ilgili mevzuat hükümlerine uygun olarak elde edilen kişisel verilerinizin Şirketimiz tarafından saklama, imha ve periyodik imha sürelerini gösterir tabloya, işbu Politika'nın Ek-2'sinde yer alan "Saklama ve İmha Süreleri Tablosu"ndan ulaşabilirsiniz.

İşbu Politika'nın Ek-2'sinde yer verilen imha sürelerinin yanında, şirketimizin kişisel verilerle ilgilenen departmanı altı aylık periyodlarla saklama süresi dolan kişisel verileri İşbu Politika'da yer verilen usullere uygun olarak imha eder. Buna göre Şirket, her yıl kişisel verilerle ilgilenen departmanı Haziran ve Ocak aylarında periyodik imha işlemini gerçekleştirir.

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.

10.DİĞER HUSUSLAR

KVKK ve ilgili diğer mevzuat hükümleri ile işbu Politika arasında uyumsuzluk olması halinde, öncelikle KVKK ve ilgili diğer mevzuat hükümleri uygulanacaktır. İşbu Politikanın basılı nüshası kişisel verilerle ilgilenen departmanı tarafından saklanır.

Şirketimiz tarafından hazırlanan işbu Politika şirkete ait www.dnbanalytics.com sitesinin faaliyete başladığı tarihten itibaren yürürlüğe girmiştir. Politikada değişiklik olması durumunda, Politikanın yürürlük tarihi ve ilgili maddeler bu doğrultuda güncellenecektir. Güncelleme tablosu Ek-3'te yer almaktadır.

Politikanın yürürlükten kaldırılmasına karar verilmesi halinde, Politikanın ıslak imzalı eski nüshaları Şirket Yönetim Kurulu'nun kararı ile kişisel veriler ile ilgilenen departmanıtarafından iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile kişisel veriler ile ilgilenen departmanıtarafından saklanır.

DNB Analytics Medya Bilişim Pazarlama Danışmanlık Hizmetleri LTD. ŞTİ

EK-1 PERSONEL UNVAN, BİRİM VE GÖREV LİSTESİ

UNVAN	BİRİM	GÖREV

EK-2 SAKLAMA VE İMHA SÜRELERİ TABLOSU

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
6098 S. TBK, 6102 S. TTK, 6502 Sayılı Tüketicinin Korunması Hakkında Kanun kapsamında saklanan veriler	- 2 Yıl - 10Yıl	- Sunulan hizmet kapsamında sözleşmenin kurulamamış olması halinde 2 yıl saklanır ve iki yıllık sürenin ardından ilk periyodik imha döneminde imha edilir. - Sözleşmenin kurulmasından sonara sözleşmenin herhangi bir şekilde sona ermesi veya sözleşmenin bitmesinden itibaren veya sözleşme konusu hizmet yargı karşısındaki bir uyuşmazlığa konu ise kesinleşmiş yargı kararının ardından 10 yıl saklanır ve on yıllık sürenin sonunda ilk periyodik imha döneminde imha edilir.
Sair İlgili mevzuat gereği toplanan veriler	İlgili Mevzuatta Öngörülen Süre Kadar	İlgili Mevzuatta Öngörülen Sürenin ardından ilk periyodik imha döneminde imha edilir.
İlgili Kişisel Verinin Türk Ceza Kanunu veya sair ceza hükmü getiren mevzuat kapsamında bir suça konu olması	Dava Zamanaşımı müddetince	Dava Zamanaşımını müteakip sürenin ardından ilk periyodik imha döneminde imha edilir.

Ticari defterler, faturalar ve ilgili kayıtların tutulması	10 yıl Saklama süresi, ticari defterlere son kaydın yapıldığı, envanterin çıkarıldığı, ara bilançonun düzenlendiği, yılsonu finansal tablolarının

	hazırlandığı ve konsolide finansal tabloların hazırlandığı, ticari yazışmaların yapıldığı veya muhasebe belgelerinin oluştuğu takvim yılının bitişiyle başlar ve 10 yılın ardından ilk periyodik imha döneminde imha edilir.
Log Kayıt Takip Sistemleri	10 yıl Saklama süresinin bitimini takip eden ilk periyodik imha süresinde imha edilir.
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	2 yıl Saklama süresinin bitimini takip eden ilk periyodik imha süresinde imha edilir.
Ziyaretçi ve Toplantı Katılımcılarının Kaydı	Etkinliğin Saklama süresinin bitimini takip eden ilk sonra periyodik imha süresinde ermesini takiben 2 yıl
Kamera Kayıtları	2 yıl Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

EK-3 GÜNCELLEME TABLOSU