KİŞİSEL VERİLERİN SAKLANMASI VE İMHA EDİLMESİ POLİTİKA BİLDİRGESİ

BURTOM ÖZEL SAĞLIK TESİSLERİ ANONİM ŞİRKETİ

İÇİNDEKİLER

BURFİZ ÖZEL SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ'nden;

KİŞİSEL VERİLERİN SAKLANMASI VE İMHA EDİLMESİ POLİTİKA BİLDİRGESİ

GİRİŞ

BURFİZ ÖZEL SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ Yönetim Kurulu'nun 07 Aralık 2021 tarih ve 2021/10 sayılı Kararıyla, bu "Kişisel Verilerin Saklanması ve İmha Edilmesi Politika Bildirgesi" kabul edilerek ilan edilmiştir

BURFİZ ÖZEL SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ Yönetim Kurulu;

BURFİZ ÖZEL SAĞLIK HİZMETLERİ ANONİM ŞİRKETİnin, tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesiyle ilgili uygulanan yöntemleri hakkında, kişisel veri işleme envanterine uygun olarak kişisel veri saklama ve imha politikasını belirleyen bu bildirgeyi ilan eder.

Kapsam
Madde 1- Bu Bildirge hükümleri, 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 7'nci maddesi ve 28 Ekim 2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümleri uyarınca, Şirket hakkında uygulanır.

Dayanak
Madde 2- Bu Bildirge, 6698 sayılı Kanunun 7 (3)'nci madde fıkrası ve 22 (1) (e) maddesinin bendi ile 28 Ekim 2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 5 (1) ve 7 (5) madde bentleri hükümlerine dayanılarak hazırlanmıştır.

Tanımlar
Madde 3 - Bu Bildirge'nin uygulanmasında,

3.1. Açık rıza: Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı,

3.2. Alıcı grubu: Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini,

3.3. Anonim hâle getirme: Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesini,

3.4. Başkan: Kişisel Verileri Koruma Kurumu Başkanı'nı,

3.5. Bildirge: BURFİZ ÖZEL SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ Kişisel Verilerin Saklanması ve İmha Edilmesi Politika Bildirgesi'ni,

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

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

3.8. İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

3.9. 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 kişileri,

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

3.11. İrtibat kişisi: Türkiye'de yerleşik olan Şirket'in ve veri sorumlusu temsilcisinin sicil kapsamındaki yükümlülükleriyle ilgili olarak, Kurul ve Kurum tarafından yapılacak iletişimlerde irtibata geçilmek üzere atanan gerçek kişiyi,

3.12. Kanun: 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanununu,

3.13. Karartma: Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle

ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması gibi işlemleri,

3.14. 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,

3.15. Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi,

3.16. Kişisel verilerin işlenmesi: 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 işlemi,

3.17. Kişisel veri işleme envanteri: Şirket'in 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,

3.18. Kişisel veri saklama ve imha politikası: Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikayı,

3.19. Kurul: Kişisel Verileri Koruma Kurulunu,

3.20. Kurum: Kişisel Verileri Koruma Kurumunu,

3.21. Maskeleme: Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde silinmesi, üstlerinin çizilmesi, boyanması ve yıldızlanması gibi işlemleri,

3.22. Periyodik imha: Kanunda yer alan kişisel verilerin işlenme 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 işlemini,

3.23. Rehber: Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi'ni,

3.24. Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicilini,

3.25. Şirket: BURFİZ ÖZEL SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ 'ini,

3.26. Veri işleyen: Şirket'in verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

3.27. Veri kategorisi: Kişisel verilerin ortak özelliklerine göre gruplandırıldığı veri konusu kişi grubu veya gruplarına ait kişisel veri sınıfını,

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

3.29. Veri konusu kişi grubu: Şirket'in kişisel verilerini işledikleri ilgili kişi kategorisini,

3.30. Veri sicil bilgi sistemi (VERBİS): Şirket'in Sicile başvuru ve Sicille ilgili diğer işlemlerde kullanacakları; internet üzerinden erişilebilen, Başkanlık tarafından oluşturulan ve yönetilen bilişim sistemini,

3.31. Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan Şirket'i,

VERİ SORUMLUSUNUN KİMLİĞİ	
Şirket Unvanı:	BURFİZ ÖZEL SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ
Adresi:	Karaman mh. Kültür cd. Biçen Sk. No:10 Nilüfer / Bursa
Mersis Numarası:	0191057206200016
Ticari Sicil Numarası:	Bursa- 75150
Resmî Web Adresi:	https://burtom.com.tr
Elektronik Posta Adresi:	burtom@burtom.com.tr
Telefon Numarası:	444 4 224

3.32. Yönerge: BURFİZ ÖZEL SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında İç Yönergesini,

3.33. Yönetim İç Yönergesi: BURFİZ ÖZEL SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ Yönetim Kurulunun 07/12/2021 tarihli ve 2021/16 sayılı Kararı ile kabul edilen Yönetim İç Yönergesini,

3.34. Yönetmelik: 28 Ekim 2017 Tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik' i ifade eder.

BİRİNCİ BÖLÜM

Kişisel Veri Saklama ve İmha Politikası

Kişisel veri saklama ve imha politikasına ilişkin esaslar
Madde 4- (1) Kanun'un 16.ncı maddesi gereğince Veri Sorumluları Siciline kayıt olmakla yükümlü olan Şirket, kişisel veri işleme envanterine uygun olarak bu Kişisel Veri Saklama ve İmha Edilmesi Politika Bildirgesi'ni hazırlamış bulunmaktadır.

(2) Kişisel veri saklama ve imha politikası hazırlanmış olması; kişisel verilerin Kanuna ve Yönetmeliğe uygun biçimde saklandığı, silindiği, yok edildiği veya anonim hale getirildiği anlamına gelmez.

Kişisel veri saklama ve imha politikasının kapsamı ile görev ve sorumluluklar
Madde 5- (1) Kişisel veri saklama ve imha politikası asgari olarak;

a) Kişisel veri saklama ve imha politikasının hazırlama amacına,
b) Kişisel veri saklama ve imha politikası ile düzenlenen kayıt ortamlarına,
i. Kayıt ortamları;

Elektronik Ortamlar	Elektronik Olmayan Ortamlar
○ Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım, vb.) ○ Yazılımlar (ofis yazılımları, portal, Kamu platformları, İntermedia, VERBİS.) ○ Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit ve engelleme, günlük kayıt dosyası, anti virüs vb.) ○ Kişisel bilgisayarlar (Masaüstü, dizüstü) ○ Mobil cihazlar (telefon, tablet vb.) ○ Optik diskler (CD, DVD vb.) ○ Çıkartılabilir bellekler (USB, Hafıza Kart vb.) ○ Yazıcı, tarayıcı, fotokopi makinesi	○ Kâğıt ○ Manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) ○ Yazılı, basılı, görsel ortamlar

c) Kişisel veri saklama ve imha politikasında yer verilen hukuki ve teknik terimlerin tanımlarına,
d) Kişisel verilerin saklanmasını ve imhasını gerektiren hukuki, teknik ya da diğer sebeplere ilişkin açıklamaya,
e) Kişisel verilerin güvenli bir şekilde saklanması ile hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi için alınmış teknik ve idari tedbirlere,
f) Kişisel verilerin hukuka uygun olarak imha edilmesi için alınmış teknik ve idari tedbirlere,
g) Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanlarına, birimlerine ve görev tanımlarına,
h) Saklama ve imha sürelerini gösteren tabloya,

ı) Periyodik imha sürelerine,

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 ve özlük verileri dışında kalan diğer özlük verileri	Hizmet akdinin devamında ve hitamından itibaren de 10 (on) yıl müddetle muhafaza edilir.

Çalışan	İşyeri Kişisel Sağlık Dosyası İçeriğindeki Veriler	Hizmet akdinin devamında ve hitamından itibaren 10(on) yıl müddetle muhafaza edilir.
İş Ortağı/Çözüm Ortağı/Danışman	İş Ortağı/Çözüm Ortağı/Danışman ile Şirket arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, İş Ortağı/Çözüm Ortağı/Danışman çalışanı verileri	İş Ortağı/Çözüm Ortağı/Danışmanın, Şirket 'le olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu md.146 ile Türk Ticaret Kanunu md.82 uyarınca 10 yıl süre ile saklanır.
Ziyaretçi	Burtom 'a ait fiziki mekâna girişte alınan Ziyaretçi 'ye ait ad, soyad, T.C. Kimlik Numarası, araç plakası ile kamera kayıtları,	2 yıl süre ile saklanır.
Aday Personel	Çalışan Adayına ait özgeçmiş ve işe başvuru formunda yer alan bilgiler	Başvuru tarihinden itibaren 2 yıldır.
Stajyer(öğrenci)	Stajyere ait staj dosyasında yer alan bilgiler	Staj ilişkisinin devamında ve hitamından itibaren 10(on) yıl müddetle muhafaza edilir.
Hasta	Hastaya ait ad, soyad, T.C. Kimlik Numarası, iletişim bilgileri, banka bilgileri, e-mail, adres, vergi numarası, vergi dairesi, ürün/hizmet tercihleri, sağlık işlem geçmişi, yeni üretilen sağlık bilgisi, özel gün bilgileri vb. bilgiler.	Hastanın satın almış olduğu her bir ürün/hizmet sunulmasından itibaren[1] en az 20 (yirmi) yıl süre ile saklanır. Vefat etmiş bir kimsenin sağlık verileri, en az 20 (yirmi) yıl süre ile saklanır.
Müşteri	Müşteri'ye ait ad, soyad, T.C. Kimlik Numarası, iletişim bilgileri, banka bilgileri, e-mail, adres, vergi numarası, vergi dairesi, ürün/hizmet tercihleri, işlem geçmişi, özel gün bilgileri vb. bilgiler.	Müşteri'nin, satın almış olduğu her bir ürün/hizmetin sunulmasından itibaren Türk Borçlar Kanunu m.146 ile Türk Ticaret Kanunu m.82 uyarınca 10 yıl süre ile saklanır.
Müşteri	Kamera görüntüleri, araç plaka bilgisi	2 yıl süre ile saklanır.
Şirket'in İş birliği İçinde Olduğu Taşeron/ Tedarikçi vb. kişilerin gerçek kişi olması halinde veya tüzel kişi olmaları halinde temsilcilerine ait kişisel bilgiler.	Şirket'in İş birliği İçinde Olduğu Taşeron/ Tedarikçi vb. ile Şirket arasındaki ticari ilişkinin yürütümüne dair kimlik bilgisi, iletişim bilgisi, finansal bilgiler, telefon numarası vb. kişisel verileri.	Şirket'in İş birliği İçinde Olduğu Taşeron/ Tedarikçi vb. olan iş/ticari ilişkisi süresince ve sona ermesinden itibaren Türk Borçlar Kanunu m.146 ile Türk Ticaret Kanunu m.82 uyarınca 10 yıl süre ile saklanır.

[1] Resmî Gazete Tarihi: 27.03.2002 Sayısı: 24708 Özel Hastaneler Yönetmeliği, "Madde 49– *Özel hastanelerde, muayene, teşhis ve tedavi amacıyla başvuran hasta, yaralı, acil ve adlî vakalar ile ilgili olarak yapılan tıbbî ve idarî işlemlere ilişkin kayıtların, düzenlenen ve kullanılan belgelerin toplanması ve bunların müteakip başvurular ile denetim ve adlî mercilerce her istenildiğinde hazır bulundurulması amacıyla tasnif ve muhafazaya uygun bir merkezî tıbbî arşiv kurulması zorunludur. (Ek cümle: RG-22/3/2017-30015) Merkezi tıbbi arşivin hastane bünyesinde bulunması zorunlu değildir. İlgili diğer mevzuat hükümleri saklı kalmak kaydıyla, özel hastanede tutulan hasta dosyaları,* ***en az yirmi yıl süre ile saklanır.***

Sağlık Bakanlığı Yönetim Hizmetleri Genel Müdürlüğü'nün internet sitesinde yayınlanan arşiv yönetmeliği ve ekindeki Yataklı ve Yataksız Tedavi Kurumlarında Yapılan Tespit ve Değerlendirme Raporunda tıbbi kayıt türlerine göre farklı arşiv süreleri belirtmiştir. Örneğin; hasta yatış, kayıt, takip ve taburculuk defterleri için 20 yıl, anestezi formları, yoğun bakım defteri, acil defteri, laboratuvar ve biyokimya tetkik defteri ile bebek tedavi defterleri için 10 yıl arşiv süresi öngörülmüşken, Ex bebek teslim defteri için 30 yıl, çocuk kayıt kartı için 15 yıl, enjeksiyon defteri için 2 yıl psikolojik görüşme kartı için 5 yıl gibi farklı saklama süreleri belirlenmiştir.

Resmi Gazete Tarih : 28/4/1937 Sayı : 3591 RADİYOLOJİ, RADİYOM VE ELEKTRİKLE TEDAVİ VE DİĞER FİZYOTERAPİ MÜESSESELERİ HAKKINDA KANUN Numarası : 3153 Madde 6 - Madde 6 – Röntgen ve radiyom ve her nevi elektrik aletleri ile tedavi ancak müessese mes'ul mütehassısı tarafından veya nezareti altında yapılır ve her tedavi seansının bitmesinden sonra her hasta için ayrı olarak tutulacak bir müşahede varakasına yapılan tedavinin nevi ve devam müddeti ve cereyanın kuvveti veya tatbik edilen radiyomun miktar ve şekli ve tedavi yapılan nahiyenin genişliği ve sair tafsilat kaydedilerek mütehassıs tarafından imza edilir. Bu müşahede kağıtları, ***en az üç sene*** *muhafaza edilir.*

Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelik 22 kez değişiklik geçirmiş olmakla birlikte yürürlükteki hali ile arşiv süresi konusunda bir de özel bir düzenleme içermemektedir."

j) Mevcut kişisel veri saklama ve imha politikasında güncelleme yapılmış ise söz konusu değişikliğe
ilişkin bilgileri kapsar.

(2) Şirket, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar;

- İnsan kaynakları süreçlerini yürütmek;
- Hastaların sağlık bilgilerini işlemek;
- Kurumsal iletişimi sağlamak;
- Şirket'in güvenliğini sağlamak;
- İstatistiksel çalışmalar yapabilmek;
- İmzalanan ticari vb. sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek;
- Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak;
- Şirket ile iş ilişkisinde bulunan gerçek/tüzel kişilerle irtibat sağlamak;
- Yasal raporlamalar yapmak ve
- İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

(3) Kişisel Verileri Saklama ve İmha Süreçlerinde Yer Alan Kişiler ve Görevleri; Şirket'in kişisel veri saklama ve imha süreçlerinde yer alan personel ve bunların görev ve sorumlulukları aşağıdaki gibidir;

Unvan		**Görev Tanımı**
Kişisel Veri Yöneticisi: Serdar Yüm Yönetim Kurulu Üyesi – İç Denetçi	:	Kanuna uyumluluk sürecinde yürütülen projelerde her türlü planlama, analiz, araştırma, risk belirleme çalışmalarını yönlendirmek; Kanun, Kişisel Verilerin İşlenmesi ve Korunması Politikası ve Kişisel Veri Saklama ve İmha Politikası uyarınca yürütülmesi gereken süreçleri yönetmek ve ilgili kişilerce gelen talepleri karara bağlamakla yükümlüdür.
Kişisel Veri Uzmanı: Elif Arabacı İnsan Kaynakları Yöneticisi	:	İlgili kişilerin taleplerinin incelenmesi ve değerlendirilmek üzere Kişisel Veri Kurulu Yöneticisine raporlanmasından; Kişisel Veri Kurulu Yöneticisi tarafından değerlendirilen ve karara bağlanan ilgili kişi taleplerine ilişkin işlemlerin Kişisel Veri Kurulu Yöneticisinin kararı uyarınca yerine getirilmesinden; saklama ve imha süreçlerinin denetiminin yapılmasından ve bu denetimlerin Kişisel Veri Kurulu Yöneticisine raporlanmasından; saklama ve imha süreçlerinin yürütülmesinden sorumludur.

İKİNCİ BÖLÜM

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi

İlkeler

Madde 6 - (1) Kanun'un 5.nci ve 6.ncı maddelerinde yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması halinde, kişisel verilerin Şirket tarafından re'sen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi gerekir.

(2) Şirket, kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesinde aşağıda belirtilen genel ilkelere uyar (Kanun m.4);

a) Hukuka 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.

Kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önleyici ve saklanmasını sağlayıcı teknik ve idari tedbirler

Madde 7 - (1) Şirket, veri güvenliğine ilişkin aşağıdaki hükümler kapsamında, gereken teknik ve idari tedbirleri almak ve ilgili mevzuat hükümlerine, Kurul kararlarına ve kişisel veri saklama ve imha politikasına uygun hareket eder (Kanun m.12):

A. Kişisel verilerin hukuka aykırı olarak işlenmesini önleyici teknik ve idari tedbirler;
a) Kişisel veri İşleme faaliyetleri, kurulan teknik sistemlerle denetlenir.
b) Alınan teknik önlemler ilgili kişiye raporlanır.
c) Kişisel veriler alanında teknik personel istihdam edilir.
ç) Kişisel veri İşleme envanterinde, kişisel verileri işleyecek ve saklayacak, personel belirlenir.
d) Şirket birimlerinin faaliyetleri analiz edilerek, bu analiz neticesinde ilgili iş birimlerinin gerçekleştirmiş olduğu kişisel veri işlemleri kayıt altına alınır.
e) Birimler arası uyumun sağlanması ve iletişimin hukuka uygun gerçekleştirilmesi için düzenlemeler yapılır, eğitimler verilir.
f) Çalışanlar, kişisel verilerin, Kişisel Verilerin Korunması Hukukuna uygun olarak ilgili düzenlemelere aykırı olacak şekilde işlenmesinin önlenmesi konusunda bilgilendirilir ve eğitilir.

B. İlgili Kişiler ve İşlenen Kişisel Veriler aşağıdadır.

KİŞİSEL VERİ KATEGORİSİ	KİŞİSELVERİ KATEGORİZASYONU AÇIKLAMA	İLGİLİ VERİ SAHİBİ
KİMLİK BİLGİSİ	TCK no, pasaport no, kimlik seri no ad-soyad, fotoğraf, doğum yeri, doğum tarihi, yaş, nüfusa kayıtlı olduğu yer, vukuatlı nüfus cüzdanı örneği	Hastalar, müşteriler, ziyaretçiler, taşeron, tedarikçi gerçek kişiler ya da tüzel kişi taşeron, tedarikçinin gerçek kişi temsilcisi, Şirket'in iş birliği içinde olduğu kurumların yetkili ve çalışanları, Şirket'in çalışanları, çalışan adayları ve üçüncü kişiler.
İLETİŞİM VERİSİ	E-mail adresi, telefon numarası, cep telefonu numarası, adres vb.	Müşteriler, hasta, taşeron, tedarikçi gerçek kişiler ya da tüzel kişi taşeron, tedarikçinin gerçek kişi temsilcisi, iş bağlantıları, potansiyel müşteriler (ve/veya onlarla ilişkili gerçek kişiler), iş ortakları, Şirket'in iş birliği içinde olduğu kurumların yetkili ve çalışanları, Burtom çalışanları, çalışan adayları ve üçüncü kişiler.

KONUM VERİSİ	Şirket araçlarının kullanımı sırasında edinilen lokasyon verileri	Yetkililer, Şirket'in iş birliği içinde olduğu kurumların yetkili ve çalışanları, Şirket çalışanları.
AİLE BİREYLERİ VE YAKIN VERİSİ	Kişisel veri sahibinin çocukları, eşleri ile ilgili kimlik bilgisi, iletişim bilgisi	Kişisel veri sahibinin çocukları, eşleri
FİZİKSEL MEKÂN GÜVENLİK BİLGİSİ	İşyeri giriş-çıkış bilgileri, görüşme kayıtları, ziyaret bilgileri, kamera kayıtları vb.	Müşteriler, hastalar, ziyaretçiler, taşeron, tedarikçi gerçek kişiler ya da tüzel kişi taşeron, tedarikçinin gerçek kişi temsilcisi, Şirket'in iş birliği içinde olduğu kurumların yetkili ve çalışanları, Burtom'un çalışanları, çalışan adayları ve üçüncü kişiler
FİNANSAL BİLGİ	Veri sahibinin yapmış olduğu işlemlerin finansal sonucunu gösteren bilgiler, banka hesap bilgileri,	Şirket çalışanları,
ÖZLÜK BİLGİSİ	Kanunen özlük dosyasına girmesi gereken her türlü bilgi ve belge (örn. Maaş miktarı, SGK primleri, bordrolar vb.)	Şirket çalışanları, çalışan adayları ve üçüncü kişiler.
ÖZEL NİTELİKLİ KİŞİSEL VERİ	Sağlık bilgisi ve adli sicil kaydı verisi	Şirket çalışanları, Hastalar.
HUKUKİ İŞLEM VE UYUM BİLGİSİ	Mahkeme veya idari merci kararları ile icra müdürlüğü belgelerinde yer alan veriler ve hukuki yükümlülükler çerçevesinde saklanması gereken belge ve kayıtlar.	Şirket çalışanları, Hastalar.
BAŞVURU/ ŞİKAYET YÖNETİMİ BİLGİSİ	Şirket'e yapılan başvuru ve/veya şikayetlerle ilgili olarak Şirket'le paylaşılan talepler ve kişisel veriler. Bunlarla ilgili kayıt ve raporlar	Tedarikçiler, iş bağlantıları, müşteriler ve/veya onlarla ilişkili gerçek kişiler, potansiyel müşteriler, Şirket'in iş birliği içinde olduğu kurumların yetkili ve çalışanları, Şirket'in çalışanları, çalışan adayları ve üçüncü kişiler.
GÖRSEL VE İŞİTSEL VERİ	Fotoğraf, kamera kayıtları.	Tedarikçiler, iş bağlantıları, müşteriler, Hastalar ve/veya onlarla ilişkili gerçek kişiler, potansiyel müşteriler, ziyaretçiler Şirket'in, iş birliği içinde olduğu kurumların yetkili ve çalışanları, Şirket'in çalışanları, çalışan adayları ve üçüncü kişiler.
TAŞIT VERİSİ	Plaka Bilgisi.	Tedarikçiler, iş bağlantıları, müşteriler ve/veya onlarla ilişkili gerçek kişiler, potansiyel müşteriler, ziyaretçiler, Burtom'un iş birliği içinde olduğu kurumların yetkili ve çalışanları, Burtom'un çalışanları, çalışan adayları ve üçüncü kişiler.
ELEKTRONİK VERİLER	Üyelik kayıtları, internet şifre parola bilgileri, IP adresi, işlem güvenliği bilgileri, log kayıtları vb.	Müşteriler,' Şirket'in iş birliği içinde olduğu kurumların yetkili ve çalışanları, ç Şirket'in alışanları, çalışan adayları, ziyaretçiler ve üçüncü kişiler (Web sitesi ziyaretçileri, Şirket'in internet erişimini kullanan kişiler vb.)
MESLEKİ VE EĞİTİM VERİLERİ	Kişinin çalıştığı kurum bilgisi, meslek odası bilgisi, sicil numarası ve diploma notu, diploma fotokopisi vb.	Tedarikçiler, iş kontakları, müşteriler ve/veya onlarla ilişkili gerçek kişiler, potansiyel müşteriler, Burtom'un iş birliği içinde olduğu kurumların yetkili ve çalışanları, Şirket'in çalışanları, çalışan adayları ve üçüncü kişiler.

SEYAHAT VERİSİ	Uçuş bilgisi, tur rotası, konaklama bilgisi vb.	Şirket'in iş birliği içinde olduğu kurumların yetkili ve çalışanları, Şirket'in çalışanları.

(2) Kişisel verilere hukuka aykırı olarak erişilmesini önleyici teknik ve idari tedbirler

a) Kişisel veri İşleme envanterinde, kişisel verilere erişebilecek personel belirlenir.
b) Şirket bünyesinde gerçekleştirilen kişisel verilere erişilme faaliyetleri, kurulan teknik sistemlerle denetlenir.
c) Erişim yetkileri sınırlandırılır ve yetkiler düzenli olarak gözden geçirilir.
d) Kişisel verilerin bulunduğu veri depolama alanlarına erişimler loglanarak uygunsuz erişimler veya erişim denemeleri ilgililere anlık olarak iletilir.
e) Çalışanlarla; eriştikleri kişisel verileri, Kanun hükümlerine aykırı olarak başkasına açıklamaması, işleme amacı dışında kullanmaması ve bu yükümlülüğün görevden ayrılmalarından sonra da devam etmesi konusunda bilgilendirilir ve bu amaçla sözleşme kurulur.

(3) Kişisel verilerin saklanmasını sağlayıcı teknik ve idari tedbirler;

a) Virüs koruma sistemleri ve güvenlik duvarlarını içeren yazılımlar ve donanımlar kullanılır.
b) Kişisel verilerin saklanmasını sağlama konusunda, teknik personele eğitim aldırılır.
c) Kişisel veri saklama faaliyetleri, kurulan teknik sistemlerle denetlenir.
d) Kişisel verilerin güvenli bir biçimde saklanmasını sağlamak amacı ile, yedekleme programları kullanılır.
e) Çalışanlar, kişisel verilerin, Kişisel Verilerin Korunması Hukukuna uygun olarak saklanması konusunda bilgilendirilir ve eğitilir.
f) Şirket, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, üstte Madde 7 (3) fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.
g) Şirket, kendi kuruluşunda, Kanun, Yönetmelik ve bu Yönerge hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapar veya yaptırır.
h) Şirket ile veri işleyen kişiler, öğrendikleri kişisel verileri Kanun, Yönetmelik ve bu Yönerge hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.
ı) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, Şirket bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.
i) 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.
j) Şirket, kişisel verilerin silinmesi, yok edilmesi, anonim hale getirilmesi işlemiyle ilgili uyguladığı yöntemleri ilgili politika ve bu Yönerge'de açıklamaktadır.
k) Şirket, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. İlgili kişinin talebi halinde, uygun yöntemi gerekçesini açıklayarak seçer.

Kişisel verilerin silinmesi
Madde 8 - (1) Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

(2) Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

(3) Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu olacak kişisel veriler belirlenir.
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcılar tespit edilir.
- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkileri ve yöntemleri tespit edilir.
- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemleri kapatılır ve ortadan kaldırılır.

(4) Kişisel verilerin silinmesi konusunda çeşitli yöntemler uygulanır: Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir. Buna ilişkin Şirket'te uygulanan yöntemler şunlardır:

a) Hizmet olarak uygulama türü bulut çözümleri (Office 365, Salesforce, Dropbox, Bilimp gibi) Bulut sisteminde veriler silme komutu verilerek silinir. Bu işlem gerçekleştirilirken ilgili kullanıcının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilir.

b) Kâğıt ortamında bulunan kişisel veriler Bu veriler için, 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.

c) Merkezi sunucuda bulunan ofis dosyaları ; Dosyanın işletim sisteminde bulunan "silme" komutu ile silinir veya dosya ya da dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim hakları kaldırılır. Bu işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda sistem yöneticisi olmadığına dikkat edilir.

d) Taşınır nitelikte medyada bulunan kişisel veriler; Flash tabanlı saklama ortamlarındaki kişisel veriler, şifreli olarak saklanır ve bu ortamlara uygun yazılımlar kullanılarak silinir.

e) Veri tabanları; Kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile (Delete vb.) silinir. Bu işlem gerçekleştirilirken ilgili kullanıcının aynı zamanda veri tabanı yöneticisi olmadığına dikkat edilir.

Kişisel verilerin yok edilmesi

Madde 9- (1) Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

(2) Şirket, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür.

(3) Kişisel verilerin yok edilmesinde çeşitli yöntemler uygulanır. Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaları tespit edilir ve verilerin bulunduğu sistemlerin türüne göre aşağıda belirtilen yöntemlerden bir ya da birkaçının kullanılmasıyla tek tek yok edilmesi gerekir:

a) Yerel sistemler

Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı kullanılabilir;

i. De - manyetize etme: Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.

ii. Fiziksel yok etme: Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. Optik veya manyetik medyayı eritmek, yakmak, toz haline getirmek ya da bir metal öğütücüden geçirmek gibi işlemlerle verilerin erişilmez kılınması sağlanır. Katı hal diskler bakımından üzerine yazma veya de-manyetize etme işlemi başarılı olmazsa, bu medyanın da fiziksel olarak yok edilmesi gerekir.

iii. Üzerine yazma: Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez o ve 1' lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir. Bu işlem özel yazılımlar kullanılarak yapılır.

b) Çevresel sistemler; Ortam türüne bağlı olarak kullanılabilecek yok etme yöntemleri aşağıda yer almaktadır;

i. Ağ cihazları (switch, router vb.): Söz konusu cihazların içindeki saklama ortamları

sabittir. Ürünler, çoğu zaman silme komutuna sahiptir, ama yok etme özelliği bulunmamaktadır. Bu sebeple, üstte (Madde 9/3.a)'da belirtilen uygun yöntemler ile yok edilir.

ii. Flash tabanlı ortamlar: Flash tabanlı sabit disklerin ATA (SATA; PATA vb.), SCSI (SCSI Expres vb.) ara yüzüne sahip olanları destekleniyorsa "block erase" komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da üstte (Madde 3.a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

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 edilir.

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 edilir.

v. Mobil telefonlar (Sim kart ve sabit hafıza alanları): Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. Üstte (Madde 3.a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

vi. Optik diskler: CD, DVD gibi veri saklama ortamlarıdır. Yakma, küçük parçalara ayırma, eritme gibi fiziksel yöntemlerle yok edilir.

vii. Veri kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimleri: Tüm veri kayıt ortamlarının söküldüğü doğrulanarak özelliğine göre üstte (Madde 9/3.a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

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. Üstte (Madde 9/3.a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

c) Kâğıt ve mikro fiş ortamları

Söz konusu ortamlardaki kişisel veriler, kalıcı ve fiziksel olarak ortam üzerine yazılı olduğundan ana ortamın yok edilmesi gerekir. Bu işlem gerçekleştirilirken ortamı kâğıt imha veya kırpma makinaları ile anlaşılmaz boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise, bulundukları elektronik ortama göre, üstte (Madde 9/3.a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

ç) 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 kopyaları yok edilir.

Yukarıdaki ortamlara ek olarak arızalanan ya da bakıma gönderilen cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise, aşağıda belirtilen şekilde gerçekleştirilir;

i. İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin üstte (Madde 9/3.a)'da belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.

ii. Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilir.

iii. Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemler alınır.

Kişisel verilerin anonim hale getirilmesi

Madde 10- (1) Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

(2) Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, Şirket, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin 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 getirilmesi gerekir.

(3) Şirket, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür. Şirket tarafından en çok kullanılan anonimleştirme teknikleri aşağıda yer almaktadır;

Değişkenleri çıkarma	İlgili kişiye ait kişisel verilerin içerisinde yer alan ve ilgili kişiyi herhangi bir şekilde tespit etmeye yarayacak doğrudan tanımlayıcıların bir ya da birkaçının çıkarılmasıdır. Bu yöntem kişisel verinin anonim hale getirilmesi için kullanılabileceği gibi, kişisel veri içerisinde veri işleme amacına uygun düşmeyen bilgilerin bulunması halinde bu bilgilerin silinmesi amacıyla da kullanılabilir.
Bölgesel gizleme	Kişisel verilerin toplu olarak anonim şekilde bulunduğu veri tablosu içinde istisna durumda olan veriye ilişkin ayırt edici nitelikte olabilecek bilgilerin silinmesi işlemidir.
Genelleştirme	Birçok kişiye ait kişisel verinin bir araya getirilip, ayırt edici bilgileri kaldırılarak istatistiki veri haline getirilmesi işlemidir.
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.

Kişisel verilerin anonim hale getirilmesi yöntemleri ve yönteminin seçilmesi
Madde 11- (1) Kişisel verilerin anonim hale getirilmesi yöntemleri

Kişisel verilerin anonim hale getirilmesinde, kişisel verilerin anonim hale getirilmesi aşamasında, Kurum'un yayınladığı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi'nde gösterilen kişisel verilerin anonim hale getirilmesi yöntemlerinden uygun olanı kullanılır.

Söz konusu Rehber kapsamında, kişisel verilerin anonim hale getirilmesi, kişisel veri saklama ve imha politikasında belirtilen esaslara uygun olarak aşağıdaki yöntemlerle gerçekleştirilir: Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup veya kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir.

Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle, anonim hale getirilmiş veriler, bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin hepsine anonim hale getirme yöntemleri adı verilir. Bu yöntemlerin uygulanması sonucunda elde edilen verilerin belirli bir kişiyi tanımlayamaz olması gerekmektedir.

Örnek alınabilecek anonim hale getirme yöntemleri aşağıda gösterilmektedir:

a) Değer düzensizliği sağlamayan anonim hale getirme yöntemleri

Değer düzensizliği sağlamayan yöntemlerde kümedeki verilerin sahip olduğu değerlerde bir değişiklik ya da ekleme, çıkartma işlemi uygulanmaz, bunun yerine kümede yer alan satır veya sütunların bütününde değişiklikler yapılır. Böylelikle verinin genelinde değişiklik yaşanırken, alanlardaki değerler orijinal hallerini korurlar. Değer düzensizliği sağlamayan anonim hale getirme yöntemlerinden bazıları aşağıda örneklerle açıklanmıştır.

i. Değişkenleri çıkartma

Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. Böyle bir durumda tablodaki bütün sütun tamamıyla kaldırılacaktır. Bu yöntem, değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin kamuya ifşa edilemeyecek kadar hassas bir veri olması veya analitik amaçlara hizmet etmiyor olması gibi sebeplerle kullanılabilir.

ii. Kayıtları çıkartma

Bu yöntemde ise veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonimlik kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır.

iii. Bölgesel gizleme; Bölgesel gizleme yönteminde de amaç veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmaktır. Belli bir kayda ait değerlerin yarattığı kombinasyon çok az görülebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabilecekse istisnai durumu yaratan değer "bilinmiyor" olarak değiştirilir.

iv. Genelleştirme; İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkânsız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir.

v. Alt ve üst sınır kodlama

Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir.

vi. Global kodlama

Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya numerik olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir. Genelde belli değerlerin öbeklenerek tahmin ve varsayımlar yürütmeyi kolaylaştırdığı hallerde kullanılır. Seçilen değerler için ortak ve yeni bir grup oluşturularak veri kümesindeki tüm kayıtlar bu yeni tanım ile değiştirilir.

vii. Örnekleme

Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur. Örnekleme yapılacak alt kümenin belirlenmesinde.

b) Değer düzensizliği sağlayan anonim hale getirme yöntemleri

Değer düzensizliği sağlayan yöntemlerle yukarıda bahsedilen yöntemlerden farklı olarak; mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma yaratılır. Bu durumda kayıtların taşıdığı değerler değişmekte olduğundan veri kümesinden elde edilmesi planlanan faydanın doğru hesaplanması gerekmektedir. Veri kümesindeki değerler değişiyor olsa bile toplam istatistiklerin bozulmaması sağlanarak hala veriden fayda sağlanmaya devam edilebilir.

i. Mikro birleştirme

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. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir.

ii. Veri değiş tokuşu

Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir.

iii. Gürültü ekleme

Bu yöntem ile seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkarmalar yapılır. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır.

c) Anonim hale getirmeyi kuvvetlendirici istatistik yöntemler

Anonim hale getirilmiş veri kümelerinde kayıtlardaki bazı değerlerin tekil senaryolarla bir araya gelmesi sonucunda, kayıtlardaki kişilerin kimliklerinin tespit edilmesi veya kişisel verilerine dair varsayımların türetilebilmesi ihtimali ortaya çıkabilmektedir. Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Bu yöntemlerdeki temel amaç, anonimliğin bozulması riskini en aza indirirken, veri kümesinden sağlanacak faydayı da belli bir seviyede tutabilmektir.

i. K-anonimlik

Anonim hale getirilmiş veri kümelerinde, dolaylı tanımlayıcıların doğru kombinasyonlarla bir araya gelmesi halinde kayıtlardaki kişilerin kimliklerinin saptanabilir olması veya belirli bir kişiye dair bilgilerin rahatlıkla tahmin edilebilir duruma gelmesi anonim hale getirme süreçlerine dair olan güveni sarsmıştır. Buna istinaden çeşitli istatistiksel yöntemlerle anonim hale getirilmiş veri kümelerinin daha güvenilir duruma getirilmesi gerekmiştir. K-anonimlik, bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilerek oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır.

ii. L-çeşitlilik; K-anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan L-çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır.

iii. T-yakınlık

L-çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır. Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denmektedir.

(2) Kişisel verilerin anonim hale getirme yönteminin seçilmesi; Şirket, yukarıdaki yöntemlerden hangilerinin uygulanacağına ellerindeki verilere bakarak karar verir. Anonim hale getirme yöntemleri uygulanırken sahip olunan veri kümesine dair aşağıdaki özelliklerin de Şirket tarafından dikkate alınır:

a) Verinin niteliği,
b) Verinin büyüklüğü,
c) Verinin fiziki ortamlarda bulunma yapısı,
ç) Verinin çeşitliliği,
d) Veriden sağlanmak istenen fayda / işleme amacı,
e) Verinin işleme sıklığı,
f) Verinin aktarılacağı tarafın güvenilirliği,
g)Verinin anonim hale getirilmesi için harcanacak çabanın anlamlı olması,
h) Verinin anonimliğinin bozulması halinde ortaya çıkabilecek zararın büyüklüğü, etki alanı,
ı) Verinin dağıtıklık / merkezilik oranı,
i) Kullanıcıların ilgili veriye erişim yetki kontrolü ve

j) Anonimliği bozacak bir saldırı kurgulanması ve hayata geçirilmesi için harcayacağı çabanın anlamlı olması ihtimali.

(3) Bir veriyi anonim hale getirdiğini düşünen Şirket, kişisel veriyi aktardığı diğer kurum ve kuruluşların bünyesinde olduğu bilinen ya da kamuya açık bilgilerin kullanılması ile söz konusu verinin yeniden bir kişiyi tanımlar nitelikte olup olmadığını, yapacağı sözleşmelerle ve risk analizleriyle kontrol etmek sorumluluğundadır. Anonimleştirme, verinin ayırt edici ve kimliği belirleyici özelliklerini yok etme işlemi olduğundan bu işlemlerin çeşitli müdahalelerle tersine döndürülmesi ve anonim hale getirilmiş verinin yeniden kimliği tespit edici ve gerçek kişileri ayırt edici hale dönüşmesi riski bulunmaktadır. Bu durum anonimliğin bozulması olarak ifade edilir. Anonim hale getirme işlemleri yalnızca manuel işlemlerle veya otomatik geliştirilmiş işlemlerle ya da her iki işlem tipinin birleşiminden oluşan melez işlemlerle sağlanabilir. Ancak, önemli olan anonim hale getirilmiş verilerin paylaşıldıktan veya ifşa edildikten sonra veriye erişebilen veya sahip olan yeni kullanıcılar tarafından anonimliğin bozulmasını engelleyecek önlemlerin alınmış olmasıdır. Anonimliğin bozulmasına dair bilinçli olarak yürütülen işlemlere "anonimliğin bozulmasına yönelik saldırılar" denilmektedir. Bu saldırılar farklı profildeki kullanıcılar tarafından farklı motivasyonlarla gerçekleşebilmektedir.

Kişisel verileri re'sen silme, yok etme veya anonim hale getirme süreleri
Madde 12- (1) Kişisel veri saklama ve imha politikası hazırlamış olan Şirket, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel verileri siler, yok eder veya anonim hale getirir.

(2) Kişisel verileri re'sen silme, yok ekme veya anonim hale getirme süreleri, Şirket Kişisel Veri İşleme Envanterinde gösterilir.

(3) Periyodik imhanın gerçekleştirileceği zaman aralığı, Şirket tarafından kişisel veri saklama ve imha politikasında belirlenir. Bu süre her halde altı ayı geçemez.

(4) Kişisel veri saklama ve imha politikası hazırlama yükümlülüğü olmayan Şirket, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden üç ay içinde, kişisel verileri siler, yok eder veya anonim hale getirir.

(5) Kurul, telafisi güç veya imkânsız zararların doğması ve açıkça hukuka aykırılık olması halinde, bu maddede belirlenen süreleri kısaltabilir.

Kişisel verileri ilgili kişinin talep etmesi durumunda silme ve yok etme süreleri
Madde 13- (1) İlgili kişi, Kanun'un 13'üncü maddesine istinaden Şirket'e başvurarak, kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde;

a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; Şirket, talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Şirket, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir.

b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa, Şirket, bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönerge kapsamında gerekli işlemlerin yapılmasını temin eder.

c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından Kanun'un 13(3) üncü madde fıkrası uyarınca, gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

(2) KVKK veya ilgili yan mevzuat hükümleri uyarınca, kişisel veri sahipleri üstteki (1) nolu fıkrada sıralanan haklarına ilişkin tüm taleplerini burtomkvkk@burtom.com.tr adresine "Kişisel Veri Başvuru Dilekçesi" başlığıyla gönderebilirler. Bu başvuruyu yaparken kişisel veri sahipleri, Burtom 'a daha önce bildirmiş oldukları ve halihazırda Burtom sisteminde kayıtlı bulunan e-posta adreslerini kullanabilir ya

da 5070 sayılı Elektronik İmza Kanunu uyarınca tanımlanmış elektronik veya mobil imza kullanabilirler.

Şirket Adı	*Mersis No.*	*Mail adresi*
BURFİZ ÖZEL SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ	0191057206200016	burtomkvkk@burtom.com.tr

ÜÇÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Kişisel verileri saklama ve imha süreçlerinde yer alanların unvanları, birimleri ve görev tanımları
Madde 14 - (1) Şirket'te kişisel verilerin; işleme araçları ve vasıtalarının belirlenmesi, veri kayıt sisteminin kurulması, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması, kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem kapsamında, göreviyle sınırlı illiyet bağı kurulan aşağıdaki birimlerin müdürleri, ve/veya şefleri ile yardımcıları sorumludurlar:

a) Mali İşler,
b) İnsan Kaynakları,
c) Bilgi İşlem,
d) Satın alma.

(2) Kişisel verileri saklama ve imha süreçlerinde yer alan üstte (1) inci fıkrada belirtilen birimlerde çalışan unvanlara sahip kişilerin; görev tanımları Yönetim İç Yönergesinde yer almaktadır.

Saklı haklar
Madde 15- Şirketimiz; Kişisel Verilerin Korunması ve İşlenmesi Politikasını değişiklik yapma hakkını saklı tutar.

Değişiklik ve ilan
Madde 16- İşbu Politikanın, yürürlüğe yeni girecek olan yasal gereklilikleri yerine getirmek adına, ancak bunlarla sınırlı kalmamak kaydıyla değiştirilmesi durumunda, ilgili metnin en güncel versiyonu web sitemizde ilan edilecektir.