Kişisel Veri Saklama ve İmha Politikası

İçindekiler

1. Amaç, Kapsam ve Tanımlar 3
1.1. Amaç 3
1.2. Kapsam 3
1.3. Tanımlar 3
2. Sorumluluk ve Görev 4
2.1. Sorumluluk ve Görev Dağılımı 4
2.2. Görevler 5
3. Saklama Ortamları 5
3.1. Dijital Ortamlar 5
3.2. Analog Ortamlar 5
4. Kişisel Verilerin Saklanması 6
4.1. Saklamanın Gerekliliği 6
4.2. Kişisel Verilerin Saklanmasındaki Hukuki Sebepler 6
4.3. Saklama Ortamlarının Belirlenmesi 6
4.4. Saklama Süresi 6
4.5. Güvenlik Tedbirleri 7
5. Kişisel Verilerin İmhası 8
5.1. Kişisel Verilerin İmhasını Gerektiren Durumlar 8
5.2. İmha Yöntemleri 8
5.3. İmha Süreleri 9
5.4. Periyodik İmha 9
5.5. İmha Sırasında Tutulması Gereken Kayıtlar 9
6. Politikada Düzenlenmeyen Durumlar 10
7. Politikanın Duyurulması ve Saklanması 10
8. Politikanın Güncellenmesi 10
8.1. Politikada Yapılan Güncellemeler 10

1. Amaç, Kapsam ve Tanımlar

1.1. Amaç

Kişisel Veri Saklama ve İmha Politikası (“Politika”), 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun 7’nci maddesinin üçüncü fıkrası ile 22’nci maddesinin birinci fıkrasının (e) bendine dayanılarak hazırlanan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmeliğin 5’nci maddesince öngörülen yükümlülüğe istinaden veri sorumlusu olarak KARTONSAN tarafından işlenen kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemleri için dayanak olması amacıyla hazırlanmıştır.

1.2. Kapsam

Bu politika, KARTONSAN’ın işleme amaçlarını ve vasıtalarını belirlediği, kurulmasından ve yönetilmesinden sorumlu olduğu dijital ya da analog veri kayıt sistemlerinde saklanan ve otomatik olan ya da olmayan yöntemlerle ilgili kişilerden elde edilen tüm kişisel veriler için uygulanır.

KARTONSAN’ın veri sorumlusu kabul edildiği her türlü kişisel veri saklama ve imha faaliyetine uygulanır.

1.3. Tanımlar

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

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

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

İlgili kişi: Kişisel verisi işlenen gerçek kişi

İlgili kişi grubu: Veri sorumlularının kişisel verilerini işledikleri ilgili kişi kategorisi

İrtibat kişisi: Türkiye’de yerleşik olan tüzel kişiler ile Türkiye’de yerleşik olmayan tüzel kişi veri sorumlusu temsilcisinin Kanun ve bu Kanuna dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile kurulacak iletişim için veri sorumlusu tarafından Sicile kayıt esnasında bildirilen gerçek kişi

Kanun: 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu

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 veri işleme 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 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 politika

Kişisel veri: Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi

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 hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem

Kişisel verilerin saklanması: Kişisel verilerin elde edilmesini takiben içeriğini, değerini veya anlamını elde edilmesinden sonraki bir zamanda tekrar işleyebilmek için veri saklamaya elverişli bir ortamda kayıt edilmesi

Kurul: Kişisel Verileri Koruma Kurulu

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 veriler ile biyometrik ve genetik veriler

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 işlemi

Sicil: Kişisel Verileri Koruma Kurumu Başkanlığı tarafından tutulan veri sorumluları sicili

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

Veri kategorisi: Kişisel verilerin ortak özelliklerine göre gruplandırıldığı veri konusu kişi grubu veya gruplarına ait kişisel veri sınıfı

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 bilişim sistemi

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan KARTONSAN

2. Sorumluluk ve Görev

2.1. Sorumluluk ve Görev Dağılımı

Bu politika kapsamındaki görevlerin belirlenmesinde sorumluluk dağılımı tabloda gösterilmiştir.

Unvan	Bölüm	Sorumluluk / Görev
Genel Müdür	Yönetim	Çalışanların bu politikaya uymalarının sağlanmasından sorumludur
Kişisel Verileri	İnsan Kaynakları ve	Bu politikanın gereklerinin belirlenmesi,

Koruma Görevlisi	Kalite Sistemleri	günün şartlarına göre gerektiğinde güncellenmesi, uygulanmasının denetlenmesi için gerekli tedbirlerin alınmasından sorumludur.
Müdürler/Yöneticiler	İlgili Departman	Amiri oldukları çalışanların politikaya uygun olarak çalışmalarının sağlanmasından sorumludur.
Çalışanlar	Tüm bölümler	Kişisel verilerin saklanmasında ve imhasında bu politikaya uygun hareket etmekle sorumludurlar.

2.2. Görevler

KARTONSAN'ın tüm bölümleri ve çalışanların görevleri:

a) Kişisel verilerin korunması konusunda yetkilendirilen kişi veya birimlerce, Politika kapsamında belirlenen kuralların, teknik ve idari tedbirlerin gereği gibi uygulanması;
b) Sorumlu oldukları bölüm varsa çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetlenmesi;
c) Kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi
ç) Kişisel verilere hukuka aykırı olarak işlenmesinin önlenmesi
d) Kişisel verilerin saklanması gerekiyorsa hukuka uygun olarak saklanmasının sağlanması amacıyla tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması ve uygulanması konusunda sorumlu birimlere yardım etmesi

3. Saklama Ortamları

3.1. Dijital Ortamlar

Bu politika kapsamında kişisel verilerin sayısallaştırılarak saklandığı ve bilişim sistemleri tarafından işlenebildiği dijital ortamlar:

a) Sunucular (Üzerinde dijital kişisel veri saklanabilen ve hizmet üretmek amacıyla (veri tabanı, e-posta, etki alanı vb.) kullanılabilen cihazlar)
b) Ağ ve bilgi güvenliği cihazları (router, firewall, switch vb.)
c) Kişisel bilgisayarlar (Masaüstü, dizüstü vb.)
ç) Mobil cihazlar (mobil telefon, tablet vb.)
d) Taşınabilir hafızalar (çıkartılabilir USB bellekler, CD/DVD, hafıza kartları)
e) Bulut
f) Kart okuyucular, kameralar

3.2. Fiziksel Ortamlar

Sayısallaştırılarak dijital ortama aktarılan ya da sayısallaştırılmayan kişisel verileri saklama amacıyla kullanılan analog ortamlar:

a) Form, defter gibi yazma araçları ile kişisel veri yazılabilecek veya baskı yoluyla elde edilmiş her türlü kişisel veri barındıran her türlü kâğıt
b) Üzerinde sayısallaştırılmadan kişisel veri saklamaya müsait kâğıt dışındaki her türlü ortam

Bir veri kayıt sisteminin parçası olmayan analog ortamlarda işlenen kişisel veriler için bu politika uygulanmaz.

4. Kişisel Verilerin Saklanması

4.1. Saklamanın Gerekliliği

Kişisel veriler ancak saklanması gerekli olduğu durumlarda uygun olan ortamda veya ortamlarda saklanabilir. Saklama dışındaki diğer kişisel veri işlemeler saklama olmadan da gerçekleştirilebiliyorsa, kişisel verilerin saklanması tercih edilemez.

Kişisel veriler, ancak Kişisel Verilerin Korunması Kanunu'nda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak saklanabilir.

Kişisel verinin saklanmasına karar verilirken

a) Hukuka ve dürüstlük kurallarına uyulması
b) Doğru ve güncel olması
c) Saklanma amacının belirli, açık ve meşru olması
ç) Saklanma amacıyla bağlantılı, sınırlı ve ölçülü olması

İlkelerine uyulmalıdır:

4.2. Kişisel Verilerin Saklanmasındaki Hukuki Sebepler

Kişisel veriler ilgili kişinin açık rızası olmaksızın saklanamaz.

İlgili kişinin açık rızası;

a) Kanunlarda açıkça öngörülmesi,
b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,
c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla sözleşmenin taraflarına ait kişisel verilerin saklanmasının gerekli olması,
ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,
d) İlgili kişinin kendisi tarafından saklanma amacına uygun amaçlar için alenileştirilmiş olması,
e) Bir hakkın tesisi, kullanılması veya korunması için saklamanın zorunlu olması
f) Veya ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için saklanmasının zorunlu olması

Durumlarında aranmaz.

4.3. Saklama Ortamlarının Belirlenmesi

Saklanması gereken kişisel verilerin saklanma ortamları belirlenirken zorunlu olan en az ortam belirlenmelidir. Kişisel verilerin elde edildiği ilk ortam saklamak için uygunsa ilk ortamdaki hali korunmalıdır. İlk hali saklanmaya uygun değilse, saklama süresi boyunca saklanmasına imkân vermiyorsa, işlenmesini zorlaştırıyorsa veya veri risk altında ise başka ortamda da saklanmasına karar verilebilir. Ortamın fiziksel özelliklerine göre kişisel verinin içeriğini en az değiştirecek biçimde saklanmalıdır. Elde edildiği ortamdan diğer bir ortama aktarımı yapılırken verinin türü değişiyorsa bu değişimin veri üzerindeki değişikliklerin azaltılması için gerekli tedbirler alınmalıdır.

4.4. Saklama Süresi

Kişisel verilerin saklanma süresi ilgili mevzuatta öngörülen süredir.
Mevzuatta herhangi bir süre öngörülmemişse saklama süresi belirlenirken

a) Kişisel verinin işlenme amacı kapsamında veri sorumlusunun faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,

b) Kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,
c) Kişisel verinin işlenme amacına bağlı olarak veri sorumlusunun elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,
ç) Kişisel verinin işlenme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,
d) Kişisel verinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,
e) Veri sorumlusunun hukuki yükümlülüğü gereği kişisel veriyi saklamak zorunda olduğu süre,
f) Veri sorumlusu tarafından kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi,

Göz önünde bulundurulmalıdır.

Saklama süreleri öncelikle kişisel verilerin kategorilerinden bağımsız olarak bulundukları bütünlük içinde değerlendirilmelidir. Bir evrak ya da belgede saklama süreleri birbirinden farklı birden fazla türde kişisel veri var ise evrak ya da belge için öngörülen saklama süresi, içerdiği kişisel veriler içinde en yüksek saklama süresidir.

Evrak ve belge üzerindeki kişisel verilerden saklama süreleri kanunla belirlenmiş olanlar için evrak ve belgedeki diğer kişisel verilerin saklama süreleri kabul edilemeyeceğinden saklama süreleri kanunla belirlenmiş kişisel verilerin silinmesi evrak ve belge imha edilmeden yerine getirilmelidir.

Saklama süreleri kişisel verilerin saklandıkları ortamlara göre farklılık gösterebilir. Bir kişisel veri hem dijital ortamda hem de analog ortamda saklanıyorsa, kişisel verinin saklama süresi bulunduğu analog ortamdaki diğer verilerle ilgili öngörülen saklama süresi kadardır. Kişisel verinin saklama süresi analog ortamın saklama süresinden daha uzun ise ve kişisel verinin bir kopyası dijital ortamda da bulunuyorsa saklama süresi evrakın saklama süresi kadardır. Sadece analog ortamda bulunuyorsa analog ortamın saklama süresi kişisel verinin saklama süresi kadar olur.

4.5. Güvenlik Tedbirleri

Veri sorumlusu kişisel verilere yetkisiz kişilerin erişiminin engellenmesi, hukuka aykırı olarak işlenmesinin engellenmesi ve muhafazasının sağlanması için gerekli tedbirleri almak zorundadır. Kişisel verilerin saklandıkları ortamlara hukuka aykırı erişimin engellenmesi için alınması gereken tedbirler teknik ve idari tedbirler olarak ayrılır.

4.5.1. Teknik ve İdari Tedbirler

a) Ağ güvenliği ve uygulama güvenliği sağlanmaktadır.
b) Ağ yoluyla kişisel veri aktarımlarında kapalı sistem ağ kullanılmaktadır.
c) Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakım kapsamındaki güvenlik önlemleri alınmaktadır.
ç) Bulutta depolanan kişisel verilerin güvenliği sağlanmaktadır.
d) Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri mevcuttur.
e) Çalışanlar için veri güvenliği konusunda belli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
f) Erişim, bilgi güvenliği, kullanım, saklama ve imha konularında kurumsal politikalar hazırlanmış ve uygulamaya başlanmıştır.
g) Gizlilik taahhütnameleri yapılmaktadır.
ğ) Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.

h) Güncel anti-virüs sistemleri kullanılmaktadır.
ı) Güvenlik duvarları kullanılmaktadır.
i) İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
j) Kişisel veri güvenliği politika ve prosedürleri belirlenmiştir.
k) Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
l) Kişisel veri güvenliğinin takibi yapılmaktadır.
m) Kişisel veri içeren fiziksel ortamların dış risklere (yangın, sel vb.) karşı güvenliği sağlanmaktadır.
n) Kişisel veriler mümkün olduğunca azaltılmaktadır.
o) Kişisel veriler yedeklenmekte ve yedeklenen kişisel verilerin güvenliği de sağlanmaktadır.
ö) Mevcut risk ve tehditler belirlenmiştir.
p) Özel nitelikli kişisel veri güvenliğine yönelik protokol ve prosedürler belirlenmiş ve uygulanmaktadır.
r) Şifreleme yapılmaktadır.

5. Kişisel Verilerin İmhası

Kişisel veriler, saklanmasını sağlayan şartların ortadan kalkması durumunda imha edilir.

a) Kişisel veri saklama ve imha politikası hazırlamış olan veri sorumlusu, 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.
b) Periyodik imhanın gerçekleştirileceği zaman aralığı altı aydır.

5.1. Kişisel Verilerin İmhasını Gerektiren Durumlar

Aşağıdaki durumlarda kişisel verilerin imhası gerekir.

5.1.1. Kurul Kararı

Kişisel verilerin işlenmesinin durdurulmasına ya da imhasına karar verilmesi durumunda diğer şartların varlığına bakılmadan kararın ilgili olduğu kişisel veriler imha edilir.

5.1.2. Açık Rızanın Geri Alınması

Kişisel veri işlemenin sadece ilgili kişinin açık rızasına bağlı olduğu durumlarda ilgili kişinin hukuka uygun bir şekilde açık rızasını geri alması durumunda başkaca bir işleme sebebinin bulunmaması durumunda kişisel veriler imha edilir.

5.1.3. İşlenme Şartlarının Ortadan Kalkması

Kanun'un 5 ve 6'ncı maddelerinde öngörülen açık rıza dışındaki işlenme şartlarının ortadan kalkması durumunda kişisel veriler imha edilir.

5.1.4. Saklama Süresinin Sona Ermesi

Bu politikada öngörülen saklama süresinin sona ermesi durumunda kişisel veriler silinir.

5.1.5. Amacın Kalmaması

Kişisel verilerin saklanmasını gerektiren amaç ya da amaçların ortadan kalkması durumunda kişisel veriler imha edilir.

5.2. İmha Yöntemleri

5.2.1. Silme

Kişisel verilerin silinmesiyle, bu verilerin tekrar hiçbir şekilde kullanılamayacak ve geri getirilemeyecek şekilde imhası amaçlanır. Kişisel veriler, kayıtlı oldukları evrak, dosya, CD, disket, hard disk gibi saklama ortamlarından geri dönüştürülemeyecek şekilde silinir.

Elektronik ortamda olan ve silme işlemi uygulanabilecek kişisel veriler silinme işlemi ile silinir.

Silme işlemi sonrasında geri getirilmesini önleyici tedbirler alınır.

Elektronik ortamda olmasına rağmen silme işlemi uygulanamayacak kişisel veriler için bulunduğu medyayı yok etme yöntemi kullanılır.

Kağıt ve benzeri fiziksel ortamda saklanan belgelerde silme işlemi kişisel verinin üstünün çıkmayacak koyu renk ile kapatılması ile gerçekleştirilir.

5.2.2. Yok Etme

Kişisel verilerin tekrar geri getirilemeyecek ve kullanılamayacak şekilde, verilerin kaydedildiği evrak, dosya, CD, disket, hard disk gibi ortamların imha edilmesidir.

Dijital ortamlarda silinme işlemi gerçekleştirilebiliyorsa yok etme yöntemi kullanılmaz. Silinme işlemenin gerçekleştirilemeyeceği optik ortamlarda ortamın çok küçük parçalara ayrılması yöntemi kullanılır.

5.2.3. Anonim Hale Getirme

Kişisel verilerin anonim hale 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 kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir.
Anonim hale getirme kararı verilirken kişisel verilerin anonim hale getirilmesindeki zorluklar göz önünde bulundurulmalı ve son çare olarak anonim hale getirme tercih edilmelidir.

5.3. İmha Süreleri

İşlenme şartları saklama sürelerinin sona ermesi ile ortadan kalkan kişisel veriler için imha süresi en fazla altı aydır.

İşlenme şartları sadece açık rızaya dayanan kişisel veriler açık rızanın ilgili kişi tarafından geri alınması durumunda 30 gün içinde imha edilir. İşlenme şartı sadece açık rıza olan ancak açık rızanın geri alınmasının dışında bir sebeple imhası öngörülen kişisel veri için imha süresi altı aydır.

İmha edilmesi konusunda Kurul kararı bulunan kişisel veriler için imha süresi 15 gündür.

5.4. Periyodik İmha

Öngörülen imha süresi periyodik imha zaman diliminden önce biten kişisel veriler periyodik imha zamanı beklenmeden imha edilirler. İmha süresi 6 ay ya da daha uzun olan kişisel veriler periyodik imha zamanında imha edilirler.

Periyodik imha süresi altı aydır. Periyodik imha, imhası gereken kişisel verilerin türlerine ve sayılarına göre bir haftalık süreye yayılabilir. Periyodik imha her yılın Temmuz ve Şubat aylarının ilk haftası gerçekleştirilir.

5.5. İmha Sırasında Tutulması Gereken Kayıtlar

Kişisel verilerin imhası sırasındaki işlemler kayıt altına alınır. İmha zamanı, imhanın periyodik olup olmadığı, imha edilen kişisel verilerin belirlenmesinde kullanılan kriterler, imha otomatik bir işlem değilse imhaya katılanların kimlikleri, imha edilen ortamlar ve kişisel veri türleri, imha işleminin sonucu ve imha süreci ile ilgili bilgi notları “Kişisel Veri İmha Formu” kayıt altına alınır. Varsa imha sürecine katılanlar ile paylaşılır.

Bu kayıtlar 3 yıl süre ile saklanır.

6. Politikada Düzenlenmeyen Durumlar

Politikada düzenlenmeyen veya Politikanın uygulanması sonucu ortaya çıkabilecek ihtilaflarda başvurulması gereken mevzuat:

a) 6698 sayılı Kişisel Verilerin Korunması Kanunu
b) 28.10.2017 tarihli Resmi Gazete'de yayınlanan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik
c) 30.12.2017 tarihli Resmi Gazete'de yayınlanan Veri Sorumluları Sicili Hakkında Yönetmelik
ç) Kişisel verilerin saklanmasında atıfta bulunulan hukuki sebeplerin yer aldığı Kanun, yönetmelik ve diğer mevzuat

7. Politikanın Duyurulması ve Saklanması

Politika çalışanlara duyurulması gereken diğer belgelerde olduğu gibi ISOkey Doküman Yönetimi Modülü ve benzeri yöntemler ile duyurulur.

8. Politikanın Güncellenmesi

Politika her yıl bir kez gözden geçirilir ve yapılması gereken değişikliklerin tespiti durumunda güncellenir. Ayrıca kişisel veri işleme envanterinde yapılan değişikliklerin politikanın güncellenmesini gerektirmesi durumlarda politika güncellenir.

8.1. Politikada Yapılan Güncellemeler

Politikada yapılan değişiklikler kayıt altına alınır.