



KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI



T.C.
KASTAMONU ÜNİVERSİTESİ
KİŞİSEL VERİ
SAKLAMA VE İMHA POLİTİKASI

Doküman No	KVKK-PO-002
İlk Yayın Tarihi	26.01.2023
Revizyon Tarihi	-
Revizyon No	00
Sayfa No	2/19

İÇİNDEKİLER

TABLolar	3
1. GİRİŞ	4
1.1. Amaç	4
1.2. Kapsam	4
1.3. Tanımlar	4
2. SORUMLULUK VE GÖREV DAĞILIMLARI	6
3. KAYIT ORTAMLARI	7
4. SAKLAMA VE İMHA İLİŞKİN AÇIKLAMALAR	7
4.1. Saklamaya İlişkin Açıklamalar	8
4.2. İmhayı Gerektiren Sebepler	9
5. TEKNİK VE İDARİ TEDBİRLER	9
5.1. Teknik Tedbirler	10
5.2. İdari Tedbirler	11
6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ	11
6.1. Kişisel Verilerin Silinmesi	12
6.2. Kişisel Verilerin Yok Edilmesi	13
6.3. Kişisel Verilerin Anonim Hale Getirilmesi	15
7. VERİ SAKLAMA SÜRESİ VE İMHA SÜRECİ	17
7.1. Saklama Süreleri	17
7.2. Periyodik İmha	17
7.3. Talep Üzerine İmha Gerektiren Durumlar	18
7.4. İmha Yönteminin Belirlenmesi	18
7.5. İmhanın Gerçekleştirilmesi	18
8. SORUMLU KİŞİLER	18
9. POLİTİKANIN YAYINLANMASI VE SAKLANMASI	18
10. POLİTİKANIN GÜNCELLEME PERİYODU	18
11. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI	19
12. GÖZDEN GEÇİRME VE ONAY TABLOSU	19

HAZIRLAYAN
Kastamonu Üniversitesi KVKK Komisyonu

ONAYLAYAN
Senato



T.C.
KASTAMONU ÜNİVERSİTESİ
KİŞİSEL VERİ
SAKLAMA VE İMHA POLİTİKASI

Doküman No	KVKK-PO-002
İlk Yayın Tarihi	26.01.2023
Revizyon Tarihi	-
Revizyon No	00
Sayfa No	3/19

TABLolar

Tablo 1 Saklama ve İmha Süreçleri Görev Dağılımı6
Tablo 2 Kişisel Veri Saklama Ortamları7
Tablo 3 Gözden Geçirme ve Onay Tablosu.....19

HAZIRLAYAN
Kastamonu Üniversitesi KVKK Komisyonu

ONAYLAYAN
Senato



T.C.
KASTAMONU ÜNİVERSİTESİ
KİŞİSEL VERİ
SAKLAMA VE İMHA POLİTİKASI

Doküman No	KVKK-PO-002
İlk Yayın Tarihi	26.01.2023
Revizyon Tarihi	-
Revizyon No	00
Sayfa No	4/19

1. GİRİŞ

1.1. Amaç

Kişisel Verileri Saklama ve İmha Politikası ("**Politika**"), 6698 Sayılı Kişisel Verileri Koruma Kanunu (**KVK Kanunu**) ve ilgili mevzuat esas alınarak Kastamonu Üniversitesi ("**Üniversite**") tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla hazırlanmıştır.

1.2. Kapsam

Üniversite çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait kişisel veriler bu Politika kapsamında olup Kastamonu Üniversitesinin sahip olduğu ya da Üniversitece yönetilen kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik faaliyetlerde bu Politika uygulanır.

1.3. Tanımlar

1.3.1. Ağ: Birden fazla bilgisayarın bilgi paylaşımı, yazılım ve donanım paylaşımı, merkezi yönetim ve destek kolaylığı gibi çeşitli sebeplerle birbirine bağlandığı yapı.

1.3.2. Ağ cihazları: Ağ yapılarını oluşturmak için kullanılan cihazlar.

1.3.3. Alıcı Grubu: Veri Sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi.

1.3.4. Açık Rıza: Belirli bir konuya ilişkin, bilgilendirmeye dayanan ve özgür iradeyle açıklanan rıza.

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

1.3.6. Bilgi güvenliği: Bilginin izinsiz veya yetkisiz bir biçimde erişim, kullanım, değiştirilme, ifşa edilme ve ortadan kaldırılmasını önlemek anlamına gelir.

1.3.7. Çalışan: Kastamonu Üniversitesi personeli.

1.3.8. ÜBYS: Üniversite Bilgi Yönetim Sistemi,

1.3.9. EBYS: Elektronik Belge Yönetim Sistemi,

1.3.10. Elektronik Ortam: Kişisel Verilerin elektronik aygıtlar ile oluşturulabileceği, okunabildiği, değiştirilebildiği ve yazılabileceği ortamlar.

1.3.11. Elektronik Olmayan Ortam: Elektronik ortamlar dışında kalan tüm yazılı, basılı, görsel vb. diğer ortamlar.

1.3.12. Hizmet Sağlayıcı: Kastamonu Üniversitesi ile belirli bir sözleşme çerçevesinde hizmet sağlayan gerçek veya tüzel kişi.

1.3.13. Üniversite/Kurum: Kastamonu Üniversitesi'ni ifade eder.

1.3.14. Bulut sistemi: Bilgisayarlar ve diğer cihazlar için, istendiği zaman kullanılabilen ve kullanıcılar arasında paylaşılan bilgisayar kaynakları sağlayan, internet tabanlı bilişim hizmetlerinin genel adıdır.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------



T.C.
KASTAMONU ÜNİVERSİTESİ
KİŞİSEL VERİ
SAKLAMA VE İMHA POLİTİKASI

Doküman No	KVKK-PO-002
İlk Yayın Tarihi	26.01.2023
Revizyon Tarihi	-
Revizyon No	00
Sayfa No	5/19

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

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

1.3.17. İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,

1.3.18. 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 gerçek veya tüzel kişileri,

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

1.3.20. KVKK: 24.03.2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nu,

1.3.21. KVK Komisyonu: Kastamonu Üniversitesi KVK Komisyonu'nu,

1.3.22. Karartma: Kişisel verilerin bütünü, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması ve buzlanması (flu hale getirilmesi) gibi işlemleri,

1.3.23. 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,

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

1.3.25. 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.

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

1.3.27. 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 ifade eder.

1.3.28. Korelasyon: İki değişken arasındaki ilişkiyi değerlendirme yöntemidir.

1.3.29. Kurul: Kişisel Verileri Koruma Kurulu'dur.

1.3.30. Log: Bilişim sistemlerinde yapılan işlemlere ilişkin elektronik ortamdaki izlerdir.

1.3.31. Manyetik medya: Manyetik veri ortamlarıdır.

1.3.32. Maskeleme: Kişisel verilerin belli alanlarının, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde boyanması ve yıldızlanması (*) gibi işlemleri ifade eder.

1.3.33. Optik medya: İçeriği dijital biçimde tutan ve bir lazer tarafından yazılan ve okunan depolama ortamlarıdır.

HAZIRLAYAN
Kastamonu Üniversitesi KVKK Komisyonu

ONAYLAYAN
Senato

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	6/19

1.3.34. 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.

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

1.3.36. Politika: Kişisel Verileri Saklama ve İmha Politikası.

1.3.37. Veri kayıt sistemi: Verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemidir.

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

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

VERBİS: Veri Sorumluları Sicil Bilgi Sistemi,

Yönetmelik: 28 Ekim 2017 tarihli Resmî Gazetede yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik.

2. SORUMLULUK VE GÖREV DAĞILIMLARI

Üniversitenin tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının artırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir. Kişisel verilerin saklama ve imha süreçlerinde görev alanların unvanları, birimleri ve görev tanımlarına ait dağılım Tablo 1'de verilmiştir.

Tablo 1 Saklama ve İmha Süreçleri Görev Dağılımı

UNVAN	BİRİM	GÖREV
Üniversite Rektörü	Üniversite Rektörlüğü	Çalışanların politikaya uygun hareket etmesinden sorumludur.
Rektör Yardımcısı	Üniversite Rektörlüğü	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Bilgi İşlem Daire Başkanı	Üniversite Rektörlüğü	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumludur.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	7/19

Kişisel Verileri Koruma İşlemleri Hazırlama ve Yürütme Komisyonu		Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Tüm Birimler ve Çalışanlar		Görevlerine ve yetkilerine uygun olarak politikanın yürütülmesinden sorumludur

3. KAYIT ORTAMLARI

İlgili kişilere ait kişisel veriler Kastamonu Üniversitesi tarafından aşağıdaki tabloda listelenen ortamlarda başta KVK Kanunu hükümleri olmak üzere ilgili mevzuata uygun olarak ve uluslararası veri güvenliği prensipleri çerçevesinde güvenli bir şekilde saklanmaktadır.

Tablo 2 Kişisel Veri Saklama Ortamları

ELEKTRONİK ORTAMLAR	ELEKTRONİK OLMAYAN ORTAMLAR
<ul style="list-style-type: none">▪ Sunucular (Etki alanı (LDAP), yedekleme, e-posta, veri tabanı, web vb.)▪ Yazılımlar (ofis yazılımları, portal vd. otomasyonlar, EBYS, ÜBYS)▪ Bilgi güvenliği araçları (günlük kayıt dosyası, antivirüs vb.)▪ Bilgisayarlar (masaüstü, dizüstü)▪ Dosya paylaşımları▪ Manyetik diskler (hard disk vb.)▪ Mobil cihazlar (telefon, tablet vb.)▪ Optik diskler (CD, DVD vb.)▪ Taşınabilir bellekler (USB, Hafıza Kartı vb.)▪ Yazıcı, tarayıcı, fotokopi makinesi▪ Kişisel Bilgisayarlar	<ul style="list-style-type: none">▪ Kâğıt▪ Manuel veri kayıt sistemleri (formlar vb.)▪ Yazılı, basılı, görsel ortamlar▪ Ofis içi alan▪ Arşiv

4. SAKLAMA VE İMHAYA İLİŞKİN AÇIKLAMALAR

Kastamonu Üniversitesi, tamamen otomatik veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlediği kişisel verileri, hukuka uygun olarak 3. Bölüm 'de belirtilen elektronik ve elektronik olmayan ortamlarda saklar ve imha eder.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	8/19

4.1. Saklamaya İlişkin Açıklamalar

Kanunun 3 üncü maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4 üncü maddesinde işlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği belirtilmiş, 5 ve 6 ncı maddelerde ise kişisel verilerin işleme şartları sayılmıştır.

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

4.1.1. Saklamayı Gerektiren Hukuki Sebepler

Kastamonu Üniversitesinde faaliyetler çerçevesinde işlenen kişisel veriler, ilgili mevzuatta öngörülen süre kadar muhafaza edilir. Bu kapsamda kişisel veriler;

- 6698 Sayılı Kişisel Verilerin Korunması Kanunu,
- 6098 Sayılı Türk Borçlar Kanunu,
- 4734 Sayılı Kamu İhale Kanunu,
- 657 Sayılı Devlet Memurları Kanunu,
- 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu,
- 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 5018 Sayılı Kamu Mali Yönetimi Kanunu,
- 6361 Sayılı İş Sağlığı ve Güvenliği Kanunu,
- 4982 Sayılı Bilgi Edinme Kanunu,
- 3071 Sayılı Dilekçe Hakkının Kullanılmasına Dair Kanun,
- 4857 Sayılı İş Kanunu,
- 2547 Sayılı Yükseköğretim Kanunu,
- 2914 Sayılı Yükseköğretim Personel Kanunu,
- 5434 Sayılı Emekli Sağlığı Kanunu,
- 2828 Sayılı Sosyal Hizmetler Kanunu
- İşyeri Bina ve Eklentilerinde Alınacak Sağlık ve Güvenlik Önlemlerine İlişkin Yönetmelik,
- Arşiv Hizmetleri Hakkında Yönetmelik
- Bu kanunlar uyarınca yürürlükte olan diğer ikincil düzenlemeler çerçevesinde öngörülen saklama süreleri kadar saklanmaktadır.

4.1.2. Saklamayı Gerektiren İşleme Amaçları

Kurum, faaliyetleri çerçevesinde işlemekte olduğu kişisel verileri aşağıdaki amaçlar doğrultusunda saklar.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------



T.C.
KASTAMONU ÜNİVERSİTESİ
KİŞİSEL VERİ
SAKLAMA VE İMHA POLİTİKASI

Doküman No	KVKK-PO-002
İlk Yayın Tarihi	26.01.2023
Revizyon Tarihi	-
Revizyon No	00
Sayfa No	9/19

- a) İnsan kaynakları süreçlerini yürütmek.
- b) Kurumsal iletişimi sağlamak.
- c) Kurum güvenliğini sağlamak,
- ç) İstatistiksel çalışmalar yapabilmek.
- d) İmzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek.
- e) VERBİS kapsamında, çalışanlar, veri sorumluları, irtibat kişileri, veri sorumlusu temsilcileri ve veri işleyenlerin tercih ve ihtiyaçlarını tespit etmek, verilen hizmetleri buna göre düzenlemek ve gerekmesi halinde güncellemek.
- f) Yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak.
- g) Kurum ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak.
- ğ) Yasal raporlamalar yapmak.
- h) Çağrı merkezi süreçlerini yönetmek.
- ı) İleride doğabilecek hukuki uyuşmazlıklarda delil olarak ispat yükümlülüğü.

4.2. İmhayı Gerektiren Sebepler

Kişisel veriler;

- a) İşlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,
- b) İşlenmesini veya saklanmasını gerektiren amacın ortadan kalkması,
- c) Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin açık rızasını geri alması,
- ç) Kanunun 11 inci maddesi gereği ilgili kişinin hakları çerçevesinde kişisel verilerinin silinmesi ve yok edilmesine ilişkin yaptığı başvurunun Üniversite tarafından kabul edilmesi,
- d) 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,
- e) 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 resen silinir, yok edilir veya anonim hale getirilir.

5. TEKNİK VE İDARİ TEDBİRLER

Kişisel verilerin güvenli bir şekilde saklanması, hukuka aykırı olarak işlenmesi ve erişilmesinin önlenmesi ile kişisel verilerin hukuka uygun olarak imha edilmesi için Kanunun 12 nci maddesiyle Kanunun 6 ncı

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	10/19

maddesi dördüncü fıkrası gereği özel nitelikli kişisel veriler için Kurul tarafından belirlenerek ilan edilen yeterli önlemler çerçevesinde Üniversite tarafından teknik ve idari tedbirler alınır.

5.1. Teknik Tedbirler

Üniversitemizde uygulanan veri güvenliği tedbirleri aşağıda belirtilmiştir:

- 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.
- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi aracılığı ile yapılmaktadır.
- Bilgi teknolojileri sistemleri tedarik, geliştirme ve bakımı kapsamındaki güvenlik önlemleri alınmaktadır.
- Çalışanlar için veri güvenliği hükümleri içeren disiplin düzenlemeleri genel hükümlere tabidir.
- Çalışanlar için veri güvenliği konusunda belirli aralıklarla eğitim ve farkındalık çalışmaları yapılmaktadır.
- Sunucu kaynaklarına erişim logları (kullanıcıların sunuculara yapmış olduğu istek logları) düzenli olarak tutulmaktadır.
- Gerektiğinde veri maskeleyme önlemi uygulanmaktadır.
- Dış paydaşlarla gizlilik taahhütnameleri yapılmaktadır. İmzalanan sözleşmeler veri güvenliği hükümleri içermektedir.
- Görev değişikliği olan ya da işten ayrılan çalışanların bu alandaki yetkileri kaldırılmaktadır.
- Kağıt yoluyla aktarılan kişisel veriler için ekstra güvenlik tedbirleri alınmakta ve ilgili evrak gizlilik dereceli belge formatında gönderilmektedir.
- Kişisel veri güvenliği sorunları hızlı bir şekilde raporlanmaktadır.
- Kurumun bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.
- Dijital ortamda kaydedilen kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.
- Kullanıcı hesap yönetimi ve yetki kontrol sistemi uygulanmakta olup bunların takibi de yapılmaktadır.
- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.
- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Kurum tarafından buna uygun bir süreç belirlenmiştir.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------



T.C.
KASTAMONU ÜNİVERSİTESİ
KİŞİSEL VERİ
SAKLAMA VE İMHA POLİTİKASI

Doküman No	KVKK-PO-002
İlk Yayın Tarihi	26.01.2023
Revizyon Tarihi	-
Revizyon No	00
Sayfa No	11/19

- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.
- Özel nitelikli kişisel veri güvenliğine yönelik protokolar belirlenmiş ve uygulanmaktadır.
- Özel nitelikli kişisel veriler elektronik posta yoluyla gönderilecekse mutlaka şifreli olarak ve KEP veya kurumsal posta hesabı kullanılarak gönderilmektedir.
- Saldırı tespit ve önleme sistemleri kullanılmaktadır.
- Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.
- Sızma (Penetrasyon) testleri ile Kurumumuz bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.
- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.
- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.
- Kurum internet sayfasına erişimde güvenli protokol (HTTPS) kullanılarak SHA 256 Bit RSA algoritmasıyla şifrelenmektedir.
- Veri işleyen hizmet sağlayıcılarının veri güvenliği konusunda belli aralıklarla denetimi sağlanmaktadır.

5.2. İdari Tedbirler

Üniversite tarafından, işlediği kişisel verilerle ilgili olarak alınan idari tedbirler aşağıda sayılmıştır:

- Çalışanların niteliğinin geliştirilmesine yönelik, kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi, kişisel verilerin muhafazasının sağlanması, iletişim teknikleri, teknik bilgi beceri, 657 sayılı Kanun ve ilgili diğer mevzuat hakkında eğitimler verilmektedir.
- Üniversite tarafından yürütülen faaliyetlere ilişkin çalışanlara gizlilik sözleşmeleri imzalatılmaktadır.
- Güvenlik politika ve prosedürlerine uymayan çalışanlara yönelik uygulanacak disiplin prosedürü genel hükümlere tabidir.
- Kişisel veri işlemeye başlamadan önce Kurum tarafından, ilgili kişileri aydınlatma yükümlülüğü yerine getirilmektedir.
- Kişisel veri işleme envanteri hazırlanmıştır.
- Kurum içi periyodik ve rastgele denetimler yapılmaktadır.
- Çalışanlara yönelik bilgi güvenliği eğitimleri verilmektedir.

6. KİŞİSEL VERİLERİ İMHA TEKNİKLERİ

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	12/19

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

6.1. Kişisel Verilerin Silinmesi

Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

6.1.1. Kişisel Verilerin Silinmesi Süreci

Kastamonu Üniversitesi'nde uygulanan kişisel veri silme süreci aşağıdaki gibidir:

- Silme işlemine konu edilecek kişisel veriler belirlenir.
- Söz konusu kişisel verinin tutulduğu ortamlar tespit edilir.
- KVK Komisyonunu, verinin tutulduğu ortamların birim sorumlularını, ilgili verinin silinmesi konusunda talimatlandırır. Birim sorumluları, dijital ortamlarda, otomasyonlarda yetkili personel; fiziki ortamlarda ise birim "İmha Komisyon"larıdır.
- Kişisel verinin silme işlemleri gerçekleştirilir.
- Kişisel verilerin silindiğine dair tutanak tutulur.

6.1.2. Kayıt Ortamlarına Göre Silme Yöntemleri

Kişisel veriler çeşitli kayıt ortamlarında saklanabildiklerinden kayıt ortamlarına uygun yöntemlerle silinmeleri gerekir:

a) Hizmet Olarak Uygulama Türü Bulut Çözümleri

Kastamonu Üniversitesi tarafından bulut sisteminde bulunan veriler silme komutu verilerek silinmelidir. Anılan işlem gerçekleştirilirken Kastamonu Üniversitesi ilgili kullanıcılarının bulut sistemi üzerinde silinmiş verileri geri getirme yetkisinin olmadığına dikkat edilmelidir.

b) Kâğıt Ortamında Bulunan Kişisel Veriler

Kâğıt ortamında bulunan kişisel veriler Kastamonu Üniversitesi tarafından karartma yöntemi kullanılarak silinmelidir. Karartma işlemi, ilgili evrak üzerindeki kişisel verilerin okunması mümkün olmayacak şekilde üzerinin çizilmesi/ boyanması şeklinde yapılır.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	13/19

c) Sunucu ve Bilgisayarlarda Yer Alan Ofis Dosyaları

Dosyanın işletim sistemindeki silme komutu ile silinmesi veya dosyanın bulunduğu dizin üzerinde ilgili kullanıcının erişim haklarının Kastamonu Üniversitesi tarafından kaldırılması (silinmesi-erişimin engellenmesi) gerekir.

ç) Taşınabilir Ortamda Bulunan Kişisel Veriler

Taşınabilir saklama ortamlarındaki kişisel veriler, şifreli olarak saklanmalı ve bu ortamlara uygun yazılımlar kullanılarak silinmelidir.

d) Veri Tabanları

Kişisel verilerin bulunduğu veri tabanı tablosundaki ilgili satır ve sütun (hücre)'lerin veri tabanı komutları ile silinmesi gerekir.

6.2. Kişisel Verilerin Yok Edilmesi

Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir.

6.2.1. 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:

a) Yerel Sistemler

Söz konusu sistemler üzerindeki verilerin yok edilmesi için aşağıdaki yöntemlerden bir ya da birkaçı Kastamonu Üniversitesi tarafından belirlenerek kullanılabilir.

- 1) De-manyetize Etme:** Manyetik medyanın özel bir cihazdan geçirilerek manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemidir.
- 2) Fiziksel Yok Etme:** İlgili verinin bulunduğu donanım/ medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemidir. İlgili verinin bulunduğu donanım/medyanın eritilmesi, yakılması, toz haline getirilmesi ya da bir metal öğütücüden geçirilmesi gibi işlemlerle verilerin erişilmez kılınması sağlanır.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	14/19

- 3) **Üzerine Yazma:** Manyetik medya ve yeniden yazılabilir optik medya üzerine rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemidir.

b) Çevresel Sistemler

Kastamonu Üniversitesi veri kayıt ortam türüne bağlı olarak kullanılabilir yok etme yöntemleri aşağıda yer almaktadır:

- Ağ cihazları (switch, router vb.):** Söz konusu donanımlar içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama yok etme özelliği bulunmamaktadır. “a” bendinde belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle ilgili verinin bulunduğu donanım/ medyanın yok edilmesi gerekir.
- Flash tabanlı ortamlar:** Flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) ara yüzüne sahip olanları, destekleniyorsa komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da (a) başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- Manyetik disk gibi üniteler:** Verileri esnek (plaka) ya da sabit ortamlar üzerindeki mikro mıknatıs parçaları yardımı ile saklayan ortamlardır. (a) başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- Mobil telefonlar (Sim kart ve sabit hafıza alanları):** Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. (a) başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.
- Optik diskler:** CD, DVD gibi veri saklama ortamlarıdır. (a) başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

c) Kâğıt 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 kırıpma makinaları ile anlaşılabilir boyutta, mümkünse yatay ve dikey olarak, geri birleştirilemeyecek şekilde küçük parçalara bölmek gerekir.

Orijinal kâğıt formattan, tarama yoluyla elektronik ortama aktarılan kişisel verilerin ise buldukları elektronik ortama göre (a) başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi gerekir.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	15/19

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 Kastamonu Üniversitesi'nin hizmet aldığı her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması gerekmektedir. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılabilir hale getirmek için gerekli şifreleme anahtarlarının tüm kopyalarının yok edilmesi gerekir.

d) Diğer Ortamlar

Yukarıdaki ortamlara ek olarak Kastamonu Üniversitesi'nin arızalanan ya da bakıma gönderilen cihazlarında yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

- 1) İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin (a) başlığında belirtilen uygun yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilmesi,
- 2) Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,
- 3) Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması gerekir.

6.3. Kişisel Verilerin Anonim Hale Getirilmesi

Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir.

Anonim hale getirme, bir veri kümesindeki tüm doğrudan ve/veya dolaylı tanımlayıcıların çıkartılarak ya da değiştirilerek, ilgili kişinin kimliğinin saptanabilmesinin engellenmesi veya bir grup/kalabalık içinde ayırt edilebilir olma özelliğini, bir gerçek kişiyle ilişkilendirilemeyecek şekilde kaybetmesidir.

Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleyme, 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.

Kişisel verilerin anonim hale getirilmesi yöntemleri ve uygulama örnekleri, Kurulun yayınlamış olduğu "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi"nde detaylı olarak açıklanmıştır.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	16/19

6.3.1. Kişisel Verilerin Anonim Hale Getirilmesi Yöntemleri

6.3.1.1. 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. Aşağıdaki yöntemlere ilişkin uygulama örnekleri, Kurulun yayınlamış olduğu “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi”nde açıklanmıştır.

- Değişkenleri Çıkartma
- Kayıtları Çıkartma
- Bölgesel Gizleme
- Alt ve Üst Sınır Kodlama
- Örneklem

6.3.1.2. Değer düzensizliği sağlayan anonim hale getirme şekilleri

Değer düzensizliği sağlayan yöntemlerle, yukarıda bahsedilen yöntemlerden farklı olarak; mevcut değerler değiştirilerek veri kümesinin değerlerinde bozulma meydana getirilir. Aşağıdaki yöntemlere ilişkin uygulama örnekleri, Kurulun yayınlamış olduğu “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi”nde açıklanmıştır.

- Mikro Birleştirme
- Veri Değiş Tokuşu
- Gürültü Ekleme
- Tekrar Örneklem

6.3.1.3. Anonim hale getirmeyi kuvvetlendirici istatistiksel 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 türetilmesi ihtimali ortaya çıkabilmektedir. Bu sebeple anonim hale getirilmiş veri kümelerinde çeşitli istatistiksel yöntemler kullanılarak veri kümesi içindeki kayıtların tekilliğini minimuma indirerek anonimlik güçlendirilebilmektedir. Aşağıdaki yöntemlere ilişkin uygulama örnekleri, Kurulun yayınlamış olduğu “Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi”nde açıklanmıştır.

- K-Anonimlik
- L-Çeşitlilik
- T-Yakınlık

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	17/19

6.3.1.4. Anonimlik Güvencesi

Bir kişisel verinin silinmesi ya da yok edilmesi yerine anonim hale getirilmesine karar verilebilmesi için aşağıdaki şartların yerine getirilmesi gereklidir. Bu şartların yerine getirilmiş olmasını veri sorumluları sağlamalıdır:

- Anonim hale getirilmiş veri kümesinin bir başka veri kümesiyle birleştirilerek anonimliğin bozulmaması,
- Bir ya da birden fazla değer bir kaydı tekil hale getirebilecek şekilde anlamlı bir bütün oluşturulmaması,
- Anonim hale getirilmiş veri kümesindeki değerlerin birleşip bir varsayım veya sonuç üretebilir hale gelmemesi.

Bu riskler sebebiyle veri sorumlularının, anonim hale getirdikleri veri kümeleri üzerinde bu maddede sıralanan özellikler değiştiğinde kontroller yapmaları ve anonimliğin korunduğundan emin olmaları gerekmektedir.

7. VERİ SAKLAMA SÜRESİ VE İMHA SÜRECİ

7.1. Saklama Süreleri

Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri “Kişisel Verileri Saklama ve İmha Sürelerini Gösterir Çizelge”de (EK-1) belirtilmiştir.

7.2. Periyodik İmha

Yönetmeliğin 11. maddesi gereğince Üniversite periyodik imha sürecini 6 ay olarak belirlemiştir. Kanunda yer alan kişisel verilerin işleme şartlarının tamamının ortadan kalkması durumunda; Kastamonu Üniversitesi işleme şartları ortadan kalkmış olan kişisel verileri işbu Kişisel Verilerin İşlenmesi ve Korunması Politikasında da belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek bir işlemle siler, yok eder veya anonim hale getirir.

Kastamonu Üniversitesi’nde kişisel verilerin saklama ve imha işlemleri, Kişisel Veri Envanterinde belirlenen sürelerde ve kamu kurumlarınca tabi olunan arşiv mevzutuna göre ilgili Komisyonların denetiminde gerçekleştirilir. Kişisel verilerin işleme şartlarını ortadan kaldıran hallerden herhangi birinin gerçekleşmesi durumunda bu kişisel verilere ilişkin kayıtlar için bir sonraki imha periyodunda imha işlemi gerçekleştirilir.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	18/19

7.3. Talep Üzerine İmha Gerektiren Durumlar

İlgili kişinin kanundan kaynaklı hakkını kullanarak yaptığı başvuruların uygun bulunması halinde veya Kişisel Verileri Koruma Kurumu'nun talimatına istinaden imha işlemi Kurum tarafından gerçekleştirilir. Veri Sorumlusu, kendisine yapılan başvuruları, KVK Komisyonu ile "Talep Yönetim Süreci Talimatı" na (EK-2) göre yürütür.

7.4. İmha Yönteminin Belirlenmesi

Kişisel Veri Envanterinde, imha edilecek kişisel verinin bulunduğu ortamın türü, kritikliği ve hassasiyetine göre Kişisel Verileri Koruma Kanununda belirtilen imha yöntemlerine göre imha türüne karar verilir.

7.5. İmhanın Gerçekleştirilmesi

İmhası gerçekleştirilecek kişisel veriler,

- 1) Belirlenen kayıtlar,
- 2) Ekipler,
- 3) Takvim ve
- 4) Yöntem dikkate alınarak gerçekleştirilir.

Veri Sorumlusu, imha edilecek kişisel verileri, veri işleyen taraflara da bildirerek ilgili taraflarda bulunan kayıtların da imhasını sağlar ve kayıt altına alır.

8. SORUMLU KİŞİLER

Kişisel verilerin saklama, silme, anonim hale getirme ve imha etme süreçleri Kastamonu Üniversitesi KVK Komisyonu tarafından yürütülür.

9. POLİTİKANIN YAYINLANMASI VE SAKLANMASI

Üniversitemiz tarafından düzenlenen ve yürürlüğe giren iş bu politika, Üniversitemiz internet sitesinde yayımlanır, internet sitesinde kamuya açıklanır. Basılı kâğıt nüshası da Genel Sekreterlik dosyasında saklanır.

10. POLİTİKANIN GÜNCELLEME PERİYODU

Politika, ihtiyaç duyuldukça gözden geçirilir ve gerekli olan bölümler güncellenir.

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------

	T.C. KASTAMONU ÜNİVERSİTESİ KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI	Doküman No	KVKK-PO-002
		İlk Yayın Tarihi	26.01.2023
		Revizyon Tarihi	-
		Revizyon No	00
		Sayfa No	19/19

11. POLİTİKANIN YÜRÜRLÜĞÜ VE YÜRÜRLÜKTEN KALDIRILMASI

Politika, Üniversite Senatosu'na kabul edildikten sonra yürürlüğe girmiş kabul edilir. Yürürlükten kaldırılmasına karar verilmesi halinde, Politika'nın ıslak imzalı eski nüshaları Senato Kararı ile iptal edilerek (iptal kaşesi vurularak veya iptal yazılarak) imzalanır ve en az 5 yıl süre ile Genel Sekreterlik tarafından saklanır.

12. GÖZDEN GEÇİRME VE ONAY TABLOSU

Tablo 3 Gözden Geçirme ve Onay Tablosu

Açıklama	Kabul/Revizyon Tarih ve Numarası	Revizyon İçeriği
İlk yayın	26/01/2023 tarihli ve 2023/02-29 sayılı Senato kararı	-

EKLER:

- 1- Kişisel Verileri Saklama ve İmha Sürelerini Gösterir Çizelge
- 2- Talep Yönetim Süreci Talimatı ve İş Akışları

HAZIRLAYAN Kastamonu Üniversitesi KVKK Komisyonu	ONAYLAYAN Senato
--	----------------------------