



## KİŞİSEL VERİ İHLALI DİSİPLİN POLİTİKASI

Doküman No	PR.KVKK.KVİD.02
Yayın Tarihi	
Revizyon Tarihi / No	
Sayfa No	1 / 5

### 1.Giriş

İşbu Kişisel Veri İhlali Disiplin Politikası (“Politika”) Belediyemiz Kişisel Verileri Koruma Kurumu (KVKK) Kişisel Veri Güvenliği Rehberi’nde yayımlanan ve veri sorumluları tarafından alınması gereken idari ve teknik tedbirler kapsamında hazırlanmıştır.

6698 sayılı Kişisel Verilerin Korunması Kanunu’nun “Veri güvenliğine ilişkin yükümlülükler” başlıklı 12’nci maddesinin (5) numaralı fıkrası “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.” hükmünü amirdir. Belediye bu amaçla, uygulanmak ve geliştirilmek üzere yazılı bir kişisel veri koruma politikası ve sistemi benimsemiştir.

### 2.Amaç

Kişisel Veri İhlali Disiplin Politikası (“Politika”), Belediyemiz tarafından gerçekleştirilen kişisel veri işleme faaliyetlerinin yürütülmesinde yaşanması muhtemel bir veri ihlalinde izlenmesi gereken politikayı ortaya koymaktadır. Belediyemiz, kişisel veri sahiplerini bilgilendirerek gerekli şeffaflığı sağlamaktadır.

### 3.Kapsam

Belediyemizin faaliyet konuları ve çalışma alanlarında kişisel verilerin işlenmesi süreçlerine dahil olan tüm bilgi sistemlerini ve alt bilgileri, sözleşmeleri, çevre ve fiziksel alanları ve tüm bunlar için üretilen sistem ve düzenlemeleri kapsamaktadır. Bu politika Belediyenin tüm birimlerini ve çalışanlarını, destek hizmeti veren firma personellerini, vatandaşları, ziyaretçileri, üçüncü kişileri, stajyer ve belediye iştraklerinde görevli personeli kapsamaktadır.

### 4.Tanımlar

Belediye	Sakarya Büyükşehir Belediyesi.
Politika	Kişisel Veri İhlali Disiplin Politikası.
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza.
Anonim Hale Getirme	Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi.
İlgili Kişi	Kişisel verisi işlenen gerçek kişi.
Kişisel veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi.
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 veriler.
Kişisel Verilerin İşlenmesi	Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi.
İlgili Kişi Başvuru Formu	6698 sayılı Kişisel Verilerin Korunması Kanunu “İlgili Kişinin Hakları” başlıklı 11. Maddesi gereğince belediyemize yapılacak başvurularda kullanılacak form.
KVKK	6698 Sayılı Kişisel Verilerin Korunması Kanunu.



## KİŞİSEL VERİ İHLALİ DİSİPLİN POLİTİKASI

Doküman No	PR.KVKK.KVİD.02
Yayın Tarihi	
Revizyon Tarihi / No	
Sayfa No	2 / 5

VERBİS	Veri Sorumluları Sicil Bilgi Sistemi
Kurul	Kişisel Verileri Koruma Kurumu Kurulu

### 5.Görev ve Sorumluluklar

Unvan	Birim	Görev	İhlale İlişkin Raporlama Yapılacak Birim
İlgili Birim de Görevli Çalışma Uyum Ekibi Personeli	İhlalin gerçekleştiği birim	Potansiyel ya da Gerçekleşen Veri İhlalinin değerlendirilmesi ve irtibat kişisine bildirilmesi.	İhlalin gerçekleştiği birim

Tablo 1: Belediye Nezdinde Veri İhlaline İlişkin Sorumlusu

#### 5.1.Verİ İhlali Müdahale Ekibi

Kişisel veri ihlali durumunda oluşan veya oluşabilecek kriz durumuna müdahale etmek ve Kanun kapsamında öngörülen yükümlülükleri yerine getirmek için aşağıda belirlenen katılımcıların dahil edileceği bir Kriz Müdahale Ekibi (Ekip) oluşturulur.

Kriz Müdahale Ekibi (Ekip) ;

- İrtibat Kişisi: Kişisel veri ihlalinin KVK Kurulu'na ve İlgili Kişiye bildirmekten sorumludur.
- İhlalin Meydana Geldiği Birimin Yöneticisi: Kişisel veri ihlali veya potansiyel veri ihlalinin analiz edilmesi ve oluşabilecek zafiyetlerin giderilerek ihlallerin tekrarlamaması için tedbir alınmasından sorumludur.
- Kişisel Verileri Koruma Kanunu Uyum Komisyonu: ihlale ilişkin Belediye nezdindeki sorumluluğun kimde olduğuna dair değerlendirmenin yapılması, kişisel veri ihlali ve potansiyel veri ihlali durumunda Veri Sorumlusu Temsilcisine bilgi vermekten sorumludur.

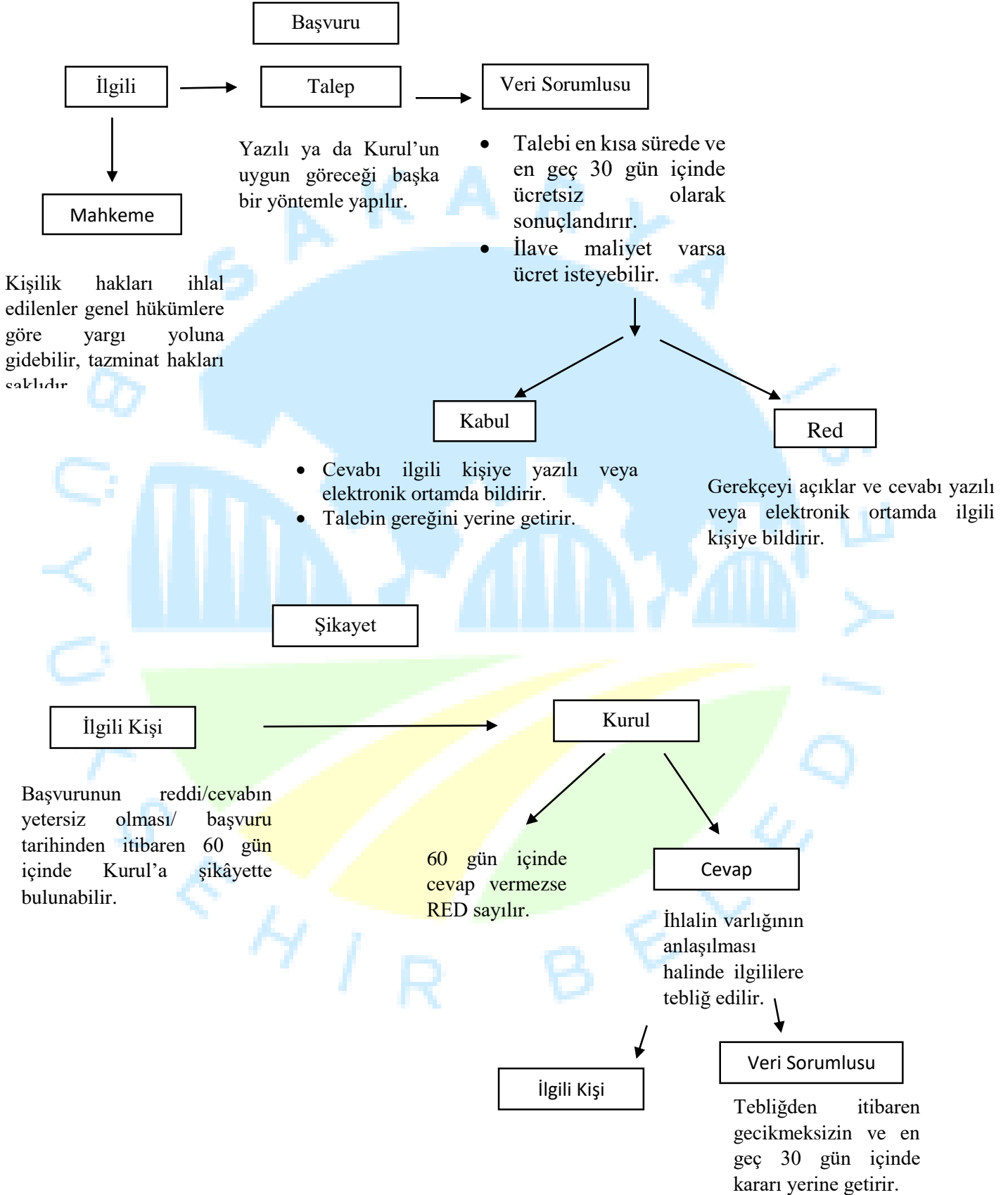
### 6. Veri İhlali'ne İlişkin Uygulanması Gereken Prosedür

#### 6.1.Başyuru Prosedürü



## KİŞİSEL VERİ İHLALİ DİSİPLİN POLİTİKASI

Doküman No	PR.KVKK.KVİD.02
Yayın Tarihi	
Revizyon Tarihi / No	
Sayfa No	3 / 5





## KİŞİSEL VERİ İHLALİ DİSİPLİN POLİTİKASI

Doküman No	PR.KVKK.KVİD.02
Yayın Tarihi	
Revizyon Tarihi / No	
Sayfa No	4 / 5

### 6.1.1.İlgili Kişiden Gelen Başvuru

İlgili kişiden gelen talep üzerine bu prosedür uygulamaya konulur. Yapılan talep üzerine araştırma yapılması için ilgili birime yönlendirilir. Yapılacak araştırmada; “Veri İhlalinin kaynağının tespiti, ihlalin ne zaman gerçekleştiği ve ne zaman tespit edilebildiği, etkilenen kişisel veri kategorilerinin (kişisel veri / özel nitelikli kişisel veri ayrımı yapılarak) tespit edilmesine ilişkin raporlama hazırlanır ve irtibat kişisine teslim edilir. İrtibat kişisi hazırlanan raporu ilgili kişiye teslim eder. İlgili birim veri ihlaline ilişkin mevcut risk ve tehditlerin belirlenmesine” ilişkin önlemler alınır.

### 6.1.2.Kuruldan Gelen Şikayet

Veri İhlali tespit edildiği anda kim tarafından tespit edildiği önemli olmaksızın bu prosedür uygulamaya konulur. Yapılan veri ihlal bildiriminde ihlale ilişkin araştırma yapılması için ilgili birime yönlendirilir. Yapılacak araştırmada; “Veri İhlalinin kaynağının tespiti, ihlalin ne zaman gerçekleştiği ve ne zaman tespit edilebildiği, etkilenen kişisel veri kategorilerinin (kişisel veri / özel nitelikli kişisel veri ayrımı yapılarak) tespit edilmesi, Veri İhlaline ilişkin mevcut risk ve tehditlerin belirlenmesine” ilişkin önlemler alınır. Olası risk ve tehditler belirlenirken aşağıdaki hususlara dikkat edilmesi gerekmektedir:

- Kişisel verilerin özel nitelikli kişisel veri olup olmadığı;
- Mahiyeti gereği hangi derecede gizlilik seviyesi gerektirdiği;
- Güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği dikkate alınmalıdır.

Bu risklerin tanımlanması ve önceliğinin belirlenmesine ilişkin raporlama yapılır. Söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik açıklanan ve aşağıda yer alan önlemler uygulamaya konulmalıdır.

#### A. Siber Güvenliğin Sağlanması:

Kişisel veri içeren bilgi teknoloji sistemlerine gelen izinsiz erişim tehditlerine karşı ilk savunma hattı olacaktır. Herhangi Potansiyel Veri İhlali veya Veri İhlali yaşanması durumunda;

- Yetkisiz erişim/saldırının belediye içinden mi yoksa belediye dışından mı yapıldığının belirlenmesi sağlanacaktır,
- Belediye sistemlerine yetkisiz erişim/saldırının halen devam edip etmediğinin belirlenmesine çalışılacaktır,
- İhlalin sebebi araştırılacaktır,
- İhlalin yaşandığı dijital ortamda, ağda yer alan dosyaların Belediye virüs programları vb. programlar vasıtasıyla taranması sağlanacaktır,
- İhlalin Belediye nezdinde yaratabileceği iş sürecine ilişkin potansiyel sorunların belirlenmesine ilişkin çalışma yapılacaktır.
- Yama yönetimi ve yazılım güncellemeleri gerçekleştirilip yazılım ve donanımların düzgün bir şekilde çalışması sağlanacaktır,
- Güvenlik duvarı yapılandırması gözden geçirilecektir,
- İhlal ile alakalı olduğu düşünülen kısımlara ilişkin şifreler ile erişim yetki ve kontrol matrisinde gerekli değişiklikler yapılacak ve gerekirse erişim yetkileri sınırlandırılacaktır.



## KİŞİSEL VERİ İHLALİ DİSİPLİN POLİTİKASI

Doküman No	PR.KVKK.KVİD.02
Yayın Tarihi	
Revizyon Tarihi / No	
Sayfa No	5 / 5

• İhlale konu olan veya suça konu veya aracı olduğu düşünülen cihazlar muhafaza edilir ve acil müdahale gerektirmeyen durumlarda üzerinde gerekli hukuki tespitler yapılmaya kadar kullanılmamalıdır.

### B. Fiziksel Veri Güvenliğinin Sağlanması:

Belediye nezdinde yaşanan Veri İhlali veya Potansiyel Veri İhlali'nin fiziksel ortamlarda meydana gelmesi halinde;

• Kişisel veri barındıran dokümanların, harddisk, Usb gibi depolama cihazlarının, diğer elektronik cihazların Belediye içinde herkese açık alanda bulunduğu anlaşılması veya çalınması halinde sorumlu birim tarafından bu evraklar sahibi/ilgilisi tespit edilene kadar sorumlu birim nezdinde üzerindeki bilgiler okunamayacak şekilde zarf veya kutu gibi kapalı bir ortamda muhafaza edilir. Muhafaza altına alınan eşyanın doküman olması durumunda bu dokümanın sahibi/ilgilisi tespit edilemediği takdirde 1 ay sonra doküman imha edilir.

• Belediye içinde kapalı olarak tutulması gereken dolap, kutu vb. gibi ortamların herkese açık şekilde bulunduğu anlaşılması halinde bu dolap ya da kutuların sahibi/ilgilisi tespit edilene kadar sorumlu birim tarafından güvenliği temin edilir.

• Belediye içinde kişisel veri barındıran herhangi bir ortamda veya bu ortamların yakınında yangın vb. gibi kişisel veri barındıran doküman yahut cihazların yok olmasına, zarar görmesine sebep olabilecek herhangi bir durum görülmesi halinde ivedilikle Belediye'nin ilgili diğer birimlerine haber verilir.

• İhlalin yaşandığı ortama ilişkin varsa kamera kayıtları incelenir, konu hakkında bilgisi olabilecek Belediyenin diğer çalışanları ile görüşülür. Gerekli görülmesi halinde konuya ilişkin bilgi ve gerekli dokümanlar hukuk müşavirliği ile paylaşılır, hukuki işlem başlatılır.

### 7. Veri İhlaline İlişkin Unsurların Kayıt Altına Alınması

Yaşanan Veri İhlaline ilişkin ihlal kaynağının tespiti, ihlalin ne zaman gerçekleştiği ve ne zaman tespit edildiği, etkilenen kişisel veri kategorilerinin tespiti kayıt altına alacak ve Kurul'un incelemesine hazır halde bulundurulacaktır.

### 8. Kurula Veri İhlali Bildirimi Yapılması

Belediye bünyesinde bir Veri İhlali yaşanması durumunda Kanun uyarınca Kurul'a 72 saat içerisinde bildirim yapılması sağlanmalıdır.

### 9. Politikanın Yürürlüğü

Politika, web sitesinde yayınlanmasının ardından yürürlüğe girmiş kabul edilir.

### 10. Politikanın Yayınlanması

Politika, Belediye internet sitesinde yayınlanarak, vatandaşlar, ziyaretçiler ve ilgili üçüncü kişilere ve Belediye çalışanlarına duyurulur.