**KİŞİSEL VERİ KAYBI PROSEDÜRÜ**

**PROSEDÜRÜN AMACI**

İşbu Prosedür 6698 sayılı Kişisel Verilerin Korunması Kanununa dayanarak düzenlenmiş olup, Bayburt Belediye Başkanlığı’nın muhafaza etmekte olduğu verilere ilişkin bir kayıp yaşanması durumunda uygulanacak hareket planını ortaya koymaktır.

Kişisel verilerin hukuka aykırı şekilde erişilmesi durumunda, Veri sorumlularının güvenilirliği ve itibarı değer kaybedeceği gibi böyle bir ihlal durumunda yetkililerin hukuki ve cezai sorumlulukları bulunmakta olduğundan, veri kaybı durumunda neler yapılması gerektiği hususunda farkındalığın yaratılması oldukça büyük önem arz etmektedir.

İşbu nedenle veri kaybı durumunda ihlalin en az zararla atlatılabilmesi için gereken önlemlerin en hızlı ve etkili şekilde alınması gerekmektedir. İşbu prosedür, veri kaybı durumunda ivedilikle uygulanması gereken hareket planını ortaya koyarak alınması gereken önlemleri içermektedir.

**PROSEDÜRÜN KAPSAMI**

İşbu prosedür, Bayburt Belediye Başkanlığı tarafından işlenen ve muhafaza edilen, otomatik, yarı otomatik veya otomatik olmayan yollarda elde edilen kişisel verileri ve özel nitelikli kişisel verileri kapsamaktadır.

İşbu prosedürde aksi belirtilmedikçe kişisel veriler ve özel nitelikli kişisel veriler birlikte “Kişisel Veriler” olarak adlandırılacaktır.

İşbu prosedür Bayburt Belediye Başkanlığı Kişisel Verilerin Korunması Politikası, Kişisel Veri Sahiplerinin Talepleri Politikası ve Veri Saklama ve İmha Politikası ile birlikte ve bu politikalara uygun olarak uygulanacaktır.

**YÜKÜMLÜLÜKLER**

Bayburt Belediye Başkanlığı çalışanları, işbu Politikada yer alan tüm hususları bilmek ve uygulamakla yükümlüdür. Buna ek olarak, Bayburt Belediye Başkanlığı çalışanları, işbu Politikada belirtilen bildirimleri belirtilen yöntemlerle ve derhal yapmakla yükümlüdür.

**VERİ KAYBI**

Kişisel Veri Kaybı, yetkili olmayan kişilerce, otomatik veya otomatik olmayan kayıt sistemlerinde tutulup tutulmadığına bakılmaksızın; erişimi sınırlandırılmış kişisel verilere erişilmesi, bu verilere Bayburt Belediye Başkanlığı tarafından erişilemez hale getirilmesi, verilerin başka bir yere gönderilmesi, başkaları tarafından ele geçirilmesi, kopyalanması, silinmesi v.b. durumları ifade etmektedir. Bu sebeple, veri kaybı ihtimalinin olduğu her durum bir kişisel veri açığı şeklinde nitelendirilmekte olup veri açığı veya veri ihlali olduğundan şüphelenilen durumlar derhal aşağıda belirtilen usule uygun olarak yetkililere bildirilmelidir. Kişisel Veri Açığı’na örnek olarak aşağıdakiler verilebilir; Kişisel veri açığı;

• Kişisel verilerin işlendiği ekipmanların kazara kaybı, belirli bir süre denetimsiz ve erişilebilir bırakılması veya çalınması (basılı evrak, laptop, sd kart, usb, akıllı telefon vb.)

• Veri veya bilgi sistemlerine yetkisiz erişim (Yetkisiz erişim elde etmek veya veri veya bilgi sistemlerinde yetkisiz değişiklik yapmak için kasıtlı veya yanlışlıkla kullanıcı oturum bilgilerini paylaşma)

• Kişisel verilerin Kanuna aykırı olarak paylaşılması (örneğin yanlış bir alıcıya gönderilen e-postalar)

• Giriş bilgileri ifşa olmuş kullanıcı hesapları (kimlik avı yoluyla kullanıcı girişi bilgilerinin deşifre edilmesi)

• Bayburt Belediye Başkanlığı’nın bilgi sistemlerine yetkisiz erişim elde etmek için başarısız veya başarılı girişimler

• Ekipman arızası,

• Zararlı yazılımların bulunması, yazılımların güncel olmaması

**VERİ KAYBI/İHLALİ/AÇIĞI DURUMUNDA YAPILACAKLAR**

Veri ihlallerinin ve ihlal sonucu oluşabilecek zararların önüne geçilebilmesi için öncelikle veri açığı olarak değerlendirilebilecek her ihtimal derhal Kişisel Veri Koruma Komitesine bildirilmelidir. Bayburt Belediye Başkanlığı içerisinde veri ihlali durumunda da veri ihlalini fark eden kişi derhal Kişisel Veri Koruma Komitesi’ne bu durumu bildirmekle yükümlüdür.

Böyle bir veri açığı veya veri ihlali durumunda, veri açığını veya veri ihlalini fark edip yetkililere bildirmeyen çalışan hakkında disiplin işlemlerinden akdin feshine kadar gidebilecek yaptırımlar uygulanabilecektir.

Veri açığı veya veri ihlali olarak değerlendirilen tüm durumlar aşağıda yer alan ekli form doldurularak derhal (……) adresine e-posta yoluyla bildirilmelidir. Bildirilen durumunun risk değerlendirmesi ihlalin ölçeği, hassasiyeti, etkilenen veri sahiplerinin sayısı ve benzeri unsurlar göz önüne alınarak Kişisel Veri Koruma Komitesi tarafından yapılacaktır. Veri sahiplerinin veri ihlali neticesinde uğrayacağı zararları önlemek, Bayburt Belediye Başkanlığı’nın itibarını ve güvenilirliğini korumak ve idari ve cezai yaptırımların önüne geçmek amacıyla önemsiz görülen durumlar dahi belirtilen yöntemlerle derhal yetkililere bildirilmelidir.

Kişisel Veri Koruma Komitesinin yapacağı risk değerlendirmesi neticesinde veri açığı veya veri ihlali ile ilgili alınacak tedbirlere ilişkin Yönetime bir rapor sunulacak olup, gerekli durumlarda ilgili savcılığa, Kurula ve diğer ilgili adli ve idari yargı organlarına tüm delillerle birlikte gerekli bildirim ve başvurular yapılacaktır.

**VERİ KAYBI VAKALARININ KAYIT ALTINA ALINMASI**

Tüm Kişisel Veri ihlalleri, bir tutanakla kayıt altına alınacak, bu tutanakta ihlalin meydana geldiği tarih ve saat, ihlalin tanımı, ihlalin meydana geldiği yer, ihlalden etkilenen kişisel veriler ve ihlalin teşkil ettiği risk bilgileri yer alacak, elektronik ve fiziki ortamdaki tüm deliller bozulmadan toplanacak ve kayıt altına alınacaktır. Veri ihlal kaydı için gerekli bilgiler Kişisel Veri Koruma Komitesi’nin gözetiminde bilgi işlem personeli veya duruma göre güvenlik personeli ile birlikte veya durumun özellik arz ettiği durumlarda dışarıdan olay tespiti ve delil toplama gibi konularda uzman olan üçüncü gerçek ve/veya tüzel kişilerden destek alınarak toplanacak, Kişisel Veri Koruma Komitesi tarafından işbu prosedüre ek İhlal Kayıt Formu’na işlenecektir.

**YÜRÜRLÜK**

İşbu Politika yayınlanma tarihi itibari ile yürürlüğe girecektir.

İşbu Politikanın tüm Belediye çalışanlarına ulaşacak biçimde yayınlanması ve gerekli güncellemelerin yapılması halinde bunların da duyurulması Kişisel Veri Koruma Komitesi’nin yükümlülüğündedir.

**EK – 1 Olay Bildirim Formu**

|  |
| --- |
| Olayı bildiren çalışanının; |
| Adı: |
| Soyadı: |
| Departmanı: |
| Olay Yeri: |
| Olay Tarihi: |
| Olay Saati: |
| Olay Tanımı (lütfen birini seçiniz):     1. Servis Dışı Bırakma Saldırısı 2. Bilgi Sızdırma 3. Zararlı Yazılım/Güncel olmayan yazılım 4. Kimlik Taklidi 5. Veritabanı Saldırısı (Sql Incejtion) 6. Oltalama (Phishing) 7. Yanlış Kişiye e-posta/mesaj gönderimi 8. Doküman Kaybı 9. Kullanıcı adı Parola Bilgilerinin Deşifre Olması 10. Hesaba İzinsiz Erişim Şüphesi 11. Ekipman kaybı 12. Diğer |
| Açıklamalar: |

**T.C BAYBURT BELEDİYE BAŞKANLIĞI**