GÜROK TURİZM VE MADENCİLİK A.Ş.
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI

Nisan 2019
İstanbul

İçindekiler

I. Politika Amaç ve Kapsamı

6102 sayılı Türk Ticaret Kanunu kapsamında bir anonim şirket olan Gürok Turizm ve Madencilik A.Ş. (bundan böyle "Gürok" olarak anılacaktır), veri sorumlusu sıfatıyla kişisel verilerin korunması ve hukuka uygun işlenmesine yönelik her türlü yasal düzenlemeye tam olarak uyum sağlamayı hedeflemektedir.

6698 sayılı Kişisel Verilerin Korunması Kanununun 16'ncı maddesi ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 5'inci maddesi kapsamında hazırlanan işbu Kişisel Veri Saklama ve İmha Politikası'nın (''Politika'') amacı, Gürok tarafından işlenen, ürün veya hizmet alan kişi, çalışanlar, aday çalışanlar ve diğer üçüncü kişilerin kişisel verilerinin, gerekli saklama sürelerini ve imha edilmelerinde uygulanacak asgari standartları belirlemektir.

İşbu Politika, veri sorumlusu Gürok'un işlediği kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi ile silme, yok etme ve anonim hale getirme işlemi için dayanak teşkil etmektedir.

İşbu Politika, Gürok'un tüm birimlerine, süreçlerine ve diğer üçüncü kişilerle iş ilişkilerine uygulanır. Bu Politika tüm Şirket yöneticilerine, çalışanlarına, danışmanlara, hizmet sağlayıcılara ya da veri toplayabilen, işleyebilen ya da verilere erişebilen (kişisel verileri ve/veya özel nitelikli kişisel verileri içeren) hizmet sağlayıcılara uygulanır.

İşbu Politika Şirket tarafından toplanan tüm kişisel verilere ve bilgilere uygulanır. İşbu Politika ile düzenlenen ve kişisel verilerin yer aldığı, elektronik ve elektronik olmayan kayıt ortamları ve/veya belgeler şunlardır:

- Sunucular (etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.)
- Yazılımlar (ofis yazılımları, portal vb.)
- 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, Blu-Ray vb.)

- Çıkartılabilir bellekler (USB, Hafıza Kart, Taşınabilir Bellek vb.)
- Yazıcı, tarayıcı, fotokopi makinesi.
- Basılı ortamdaki bilgi ve belgeler,
- Video ve ses kayıtları,
- Fiziksel erişim kontrol sistemleri tarafından üretilen veriler.

II. İlgili Mevzuat ve Diğer Belgeler

- 6698 sayılı Kişisel Verilerin Korunması Kanunu
- 28 Ekim 2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik
- 30 Aralık 2017 tarihli Veri Sorumluları Sicili Hakkında Yönetmelik
- 10 Mart 2018 tarihli Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ

- 6098 sayılı Türk Borçlar Kanunu
- 4857 sayılı İş Kanunu
- 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu
- 6361 sayılı İş Sağlığı ve Güvenliği Kanunu
- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

- Gürok Kişisel Verilerin Korunması ve İşlenmesi Politikası
- Gürok Özel Nitelikli Kişisel Verilerin İşlenmesi Politikası
- Gürok Temiz Masa & Temiz Ekran Politikası
- Gürok KVKK İlgili Kişi Başvuru Prosedürü
- Gürok Çalışan İletişim & BT Araçları Kullanım ve Denetleme Prosedürü

III. Tanımlar

Bu Politika'da yer alan terimler, aşağıda yer verilen anlamları ifade eder.

Tanım	Açıklama
Alıcı Grubu	Veri sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisi
Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza
Anonim Hâle Getirme	Kişisel verilerin, başka verilerle eşleştirilerek kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesi
İlgili Kişi	Kişisel verisi işlenen gerçek kişi
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
Kanun veya KVKK	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	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi
Kişisel Veri İşleme Envanteri	Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri 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 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.
Kurul	Kişisel Verileri Koruma Kurulu
Kurum	Kişisel Verileri Koruma Kurumu
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
Periyodik İmha	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 işlemidir.
Şirket veya Gürok	Gürok Turizm ve Madencilik Anonim Şirketi
Veri İşleyen	Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemi
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi

Veri Sorumluları Sicil Bilgi Sistemi (VERBİS)	Veri sorumlularının Sicile başvuruda ve Sicile ilişkin ilgili diğer işlemlerde kullanacakları, internet üzerinden erişilebilen, Kurum tarafından oluşturulan ve yönetilen bilişim sistemi.
Yönetmelik	28 Ekim 2017 tarihli Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik

IV. Genel Saklama Prensipleri

Saklama Süresi

Şirket, kişisel veri saklama süresi boyunca saklanması gereken belgeler ve elektronik kayıtlar için süre tanımını Ek-1'de yer alan Saklama ve İmha Süreleri Tablosu'nda yapar ve günceller.

Bu Politika ve eklerinde aksi belirtilmedikçe, Şirket Kişisel Veri İşleme Envanteri'ndeki veri kategorilerinde yer alan kişisel veriler, kural olarak ilgili kişisel verinin elde edildiği tarihten itibaren Ek-1'de belirtilen süreler ile saklanır.

İstisnai olarak, veri saklama süreleri aşağıdaki durumlarda uzatılabilir:

- Resmi mercilerce yürütülen soruşturma veya araştırmalarda talep edilmesi halinde ve/veya Şirket'in hukuki yükümlülüğü veya yasal haklarının gerektirdiği hallerde;

- Yargılama veya sair yasal süreçlerinde yürürlükteki mevzuat kapsamındaki hakların kullanılması için gerektiği hallerde.

Kişisel verilerin işlendikleri amaç için gerekli olan azami muhafaza edilme süresi belirlenirken;

- İlgili veri kategorisinin işlenme amacı kapsamında Şirket'in faaliyet gösterdiği sektörde genel teamül gereği kabul edilen süre,

- İlgili veri kategorisinde yer alan kişisel verinin işlenmesini gerekli kılan ve ilgili kişiyle tesis edilen hukuki ilişkinin devam edeceği süre,

- İlgili veri kategorisinin işlenme amacına bağlı olarak Şirket'in elde edeceği meşru menfaatin hukuka ve dürüstlük kurallarına uygun olarak geçerli olacağı süre,

- İlgili veri kategorisinin işlenme amacına bağlı olarak saklanmasının yaratacağı risk, maliyet ve sorumlulukların hukuken devam edeceği süre,

- Belirlenecek azami sürenin ilgili veri kategorisinin doğru ve gerektiğinde güncel tutulmasına elverişli olup olmadığı,

- Şirket'in hukuki yükümlülüğü gereği ilgili veri kategorisinde yer alan kişisel verileri saklamak zorunda olduğu süre,

- Şirket tarafından, ilgili veri kategorisinde yer alan kişisel veriye bağlı bir hakkın ileri sürülmesi için belirlenen zamanaşımı süresi,

dikkate alınır.

Şirket, kişisel verilerin işlendikleri amaç için gerekli olan azami süreleri belirlerken ve uygularken, söz konusu sürelerin Şirket Kişisel Veri İşleme Envanteri'nde yer alan bilgilerle uyumunu ve azami sürelerin aşılıp aşılmadığını takip eder. Şirket tarafından, faaliyetleri kapsamında işlenmekte olan kişisel verilerle ilgili olarak;

- Süreçlere bağlı olarak gerçekleştirilen faaliyetler kapsamındaki tüm kişisel verilerle ilgili kişisel veri bazında saklama süreleri Kişisel Veri İşleme Envanterinde;
- Veri kategorileri bazında saklama süreleri VERBİS'e kayıtta;
- Süreç bazında saklama süreleri ise Kişisel Veri Saklama ve İmha Politikasında

yer alır.

Söz konusu saklama süreleri üzerinde, gerekmesi halinde güncellemeler yapılır. Saklama süreleri sona eren kişisel veriler için re'sen silme, yok etme veya anonim hale getirme işlemi tatbik edilir.

Saklama Kuralları ve Tedbirler

Kişisel verilerin saklanması sürecinde, ilgili kişisel verinin saklama veya arşivleme için kullanılan veri ortamının (yazılı, dijital vb.) yıpranma ihtimali göz önünde bulundurulur. Eğer kişisel verilerin elektronik ortamda depolama yöntemi ile saklanması seçilmiş ise, ağ bileşenleri arasında saklama süresince sınırlı ve sadece yetkili kişilerce erişim sağlanır.

Şirket'te yer alan cihazlarda ya da kâğıt ortamında saklanan kişisel veriler, bu cihazların ve kağıtların çalınması veya kaybolması gibi tehditlere karşı fiziksel güvenlik önlemlerinin alınması suretiyle korunur. Aynı şekilde, kişisel verilerin yer aldığı fiziksel ortamlar da dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunur. Bu ortamlara giriş / çıkışlar kontrol altına alınır.

Aynı seviyedeki önlemler, Şirket dışında yer alan ve Şirket' ait kişisel veri içeren kâğıt ortamları, elektronik ortam ve cihazlar için de alınır.

Şirket'in işlenen kişisel verilerin güvenliğine yönelik almış olduğu tedbirlere aşağıda yer verilmektedir:

- Şirket tarafından, sızma testleri ile bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.

- Bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler Şirket tarafından sürekli olarak izlenmektedir.

- Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile güvenlik tanımları aracılığı ile yapılmaktadır.

- Şirketin bilişim sistemleri teçhizatı, yazılım ve verilerin fiziksel güvenliği için gerekli önlemler alınmaktadır.

- 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.

- Kişisel verilerin hukuka aykırı işlenmesini önlemeye yönelik riskler belirlenmekte, bu risklere uygun teknik tedbirlerin alınması sağlanmakta ve alınan tedbirlere yönelik teknik kontroller yapılmaktadır.

- Şirket içerisinde erişim prosedürleri oluşturularak kişisel verilere erişim ile ilgili raporlama ve analiz çalışmaları yapılmaktadır.

- Kişisel verilerin bulunduğu saklama alanlarına erişimler kayıt altına alınarak uygunsuz erişimler veya erişim denemeleri kontrol altında tutulmaktadır.

- Şirket, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli tedbirleri almaktadır.

- Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurula bildirmek için Şirket tarafından EK-2'deki prosedür hazırlanmış ve buna uygun bir sistem ve altyapı oluşturulmuştur.

- Güvenlik açıkları takip edilerek uygun güvenlik yamaları yüklenmekte ve bilgi sistemleri güncel halde tutulmaktadır.

- Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.

- Kişisel verilerin işlendiği elektronik ortamlarda güvenli kayıt tutma (loglama) sistemleri kullanılmaktadır.

- Kişisel verilerin güvenli olarak saklanmasını sağlayan veri yedekleme programları kullanılmaktadır.

- Elektronik olan veya olmayan ortamlarda saklanan kişisel verilere erişim, erişim prensiplerine göre sınırlandırılmaktadır.

- Özel nitelikli kişisel verilerin güvenliğine yönelik, "**Özel Nitelikli Kişisel Verilerin İşlenmesi Politikası**" adıyla ayrı bir politika belirlenmiştir.

V. Bilgi Güvenliği Tedbirleri

Şirket bünyesinde, bilgi güvenliğine yönelik önlem, tedbir ve atılacak adımlara ilişkin olarak aşağıdaki politika ve prosedürler tanzim edilmiş ve Şirket Yönetim Kurulu tarafından onaylanarak yürürlüğe konulmuştur:

Politikalar:

1- Bilgi Güvenliği Politikası
2- Erişim Kontrol Politikası
3- Network Politikası
4- Kriptografik Kontroller ve Anahtar Yönetimi Politikası
5- Güvenli Sistem Geliştirme Politikası
6- Uzaktan Çalışma Politikası
7- Teçhizat ve Medya Güvenliği Politikası
8- Kabul Edilebilir Kullanım Politikası
9- Bilgi Değişim Politikası
10- Parola Yönetimi Politikası
11- Fiziksel ve Çevresel Güvenlik Politikası
12- Ayrıcalık Hakları Yönetimi Politikası

Prosedürler

1- Varlık Yönetimi Prosedürü
2- Olay İhlal Yönetimi Prosedürü
3- BT Proje Yönetim Prosedürü
4- Sosyal Medya Kullanım Prosedürü

Form ve Sair Belgeler

1- Veri İmha Formu
2- Erişim Yetki Matrisi
3- Şirket Bilgisayarı Tahsis ve Kullanım Talimatı
4- Şirket Hattı ve Telefonu Tahsis ve Kullanım Talimatı

VI. Kişisel Verilerin İmhası

Genel Olarak Kişisel Verilerin İmha Şartları

Kişisel verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler, resen veya ilgili kişinin talebi üzerine Şirket tarafından silinir, yok edilir veya anonim hale getirilir. Buna göre;

- Kişisel verileri işlemeye esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası,

- Şirket ile ilgili kişi arasındaki sözleşmenin hiç kurulmamış olması, sözleşmenin geçerli olmaması, sözleşmenin kendiliğinden sona ermesi, sözleşmenin feshi veya sözleşmeden dönülmesi,

- Kişisel verilerin işlenmesini gerektiren amacın ortadan kalkması,

- Kişisel verileri işlemenin hukuka veya dürüstlük kuralına aykırı olması,

- Kişisel verileri işlemenin sadece açık rıza şartına istinaden gerçekleştiği hallerde, ilgili kişinin rızasını geri alması,

- İlgili kişinin, Kanunun 11. maddesinin (e) ve (f) bentlerindeki hakları çerçevesinde kişisel verileri işleme faaliyetine ilişkin yaptığı başvurunun Şirket tarafından kabul edilmesi,

- Şirket'in, ilgili kişi tarafından kişisel verilerinin silinmesi veya yok edilmesi talebi ile kendisine yapılan başvuruyu reddetmesi, verdiği cevabın yetersiz bulunması veya Kanunda öngörülen süre içinde cevap vermemesi hallerinde; Kurula şikâyette bulunulması ve bu talebin Kurul tarafından uygun bulunması,

- Kişisel verilerin saklanmasını gerektiren azami sürenin geçmiş olmasına rağmen, kişisel verileri daha uzun süre saklamayı haklı kılacak herhangi bir şartın mevcut olmaması,

- Kanunun 5 ve 6. maddelerindeki kişisel verilerin işlenmesini gerektiren şartların ortadan kalkması,

hallerinde kişisel verilerin silinmesi, yok edilmesi ya da anonim hâle getirilmesi gerekir.

Kişisel Verilerin İmha Teknikleri

Kişisel verilerin silinmesi; söz konusu kişisel verilerin ilgili kullanıcılar tarafından hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. Şirket, silinen kişisel verilerin ilgili kullanıcılar tarafından erişilemez ve tekrar kullanılamaz olmasını temin eder.

Şirket tarafından kişisel verilerin silinmesi işleminde aşağıdaki süreç tatbik edilir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi;

- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için ilgili kullanıcıların tespit edilmesi;

- İlgili kullanıcıların erişim, geri getirme, tekrar kullanma gibi yetkilerinin ve yöntemlerinin tespit edilmesi;

- İlgili kullanıcıların kişisel veriler kapsamındaki erişim, geri getirme, tekrar kullanma yetki ve yöntemlerinin kapatılması ve ortadan kaldırılması.

Kayıt ortamlarına göre kişisel veriler aşağıdaki şekilde silme işlemine tabi tutulur:

- Sunucularda yer alan kişisel verilerden, saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.

- Elektronik ortamda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, veri tabanı yöneticisi hariç diğer çalışanlar (ilgili kullanıcılar) için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

- Fiziksel ortamda tutulan kişisel verilerden saklanmasını gerektiren süre sona erenler için evrak arşivinden sorumlu birim yöneticisi hariç diğer çalışanlar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir. Ayrıca, üzeri okunamayacak şekilde çizilerek/boyanarak/silinerek karartma işlemi de uygulanır.

- Taşınabilir medyada bulunan kişisel verilerden saklanmasını gerektiren süre sona erenler, sistem yöneticisi tarafından şifrelenerek ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

Yok etme; bilgilerin saklandığı veri saklamaya elverişli tüm fiziksel kayıt ortamlarının tekrar geri getirilemeyecek ve kullanılamayacak hale getirilmesidir.

Kayıt ortamlarına göre kişisel veriler aşağıdaki şekilde yok etme işlemine tabi tutulur:

- Kâğıt ortamında yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler, kâğıt kırpma makinelerinde geri döndürülemeyecek şekilde yok edilir.

- Optik medya ve manyetik medyada yer alan kişisel verilerden saklanmasını gerektiren süre sona erenlerin eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesi işlemi uygulanır. Ayrıca, manyetik medya özel bir cihazdan geçirilerek yüksek değerde manyetik alana maruz bırakılması suretiyle üzerindeki veriler okunamaz hale getirilir.

Kişisel verilerin anonim hale getirilmesi; kişisel verilerin başka verilerle eşleştirilse dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. Bu kapsamda, veri üzerinden bir izleme yapılarak başka verilerle eşleştirme ve destekleme sonrasında verinin kime ait olduğu anlaşılabiliyorsa, bu verinin anonim hale getirildiği kabul edilemez.

Anonimleştirilen veri artık kişisel veri niteliklerine sahip olmayacağından, Kanun hükümlerine tabi olamayacaktır. Veri setleri anonimleştirme işlemlerine tabi tutuldukları ana kadar kişisel veri niteliklerine sahip olduklarından, bu veriler

üzerinde gerçekleştirilecek her türlü işlem kişisel verilerin işlenmesi olarak kabul edilmektedir.

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.

Periyodik İmha

Gürok bünyesinde işlenen kişisel veriler, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 11'inci maddesi uyarınca, ilgili takvim yılının ilk günü itibariyle 6 (altı) ayda bir periyodik imha işlemine tabi tutulur.

İşbu Politika kapsamında, kişisel verileri silme, yok etme veya anonim hale getirme yükümlülüğünün ortaya çıktığı tarihi takip eden ilk periyodik imha işleminde, kişisel veriler silinir, yok edilir veya anonim hale getirilir.

İlgili kişinin, KVKK'nın 13'üncü maddesine istinaden Şirket'e başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep etmesi halinde;

- 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.

- 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 Politika ve ilgili mevzuat kapsamında gerekli işlemlerin yapılmasını temin eder.

- Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep Şirket tarafından Kanunun 13'üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir.

VII. Politika Sorumluları

İşbu Politika'nın hazırlanması, güncellenmesi ve uygulanmasından Şirket bünyesinde kişisel verilerin tutulduğu, işlendiği ve/veya aktarıldığı sistemleri kullanan/yöneten birimler ve ilgili çalışanlar sorumludur. Bu bağlamda Şirket'in tüm birimleri ve çalışanları, sorumlu birimlerce Politika kapsamında alınmakta olan teknik ve idari tedbirlerin gereği gibi uygulanması, birim çalışanlarının eğitimi ve farkındalığının arttırılması, izlenmesi ve sürekli denetimi ile kişisel verilerin hukuka aykırı olarak işlenmesinin önlenmesi, kişisel verilere hukuka aykırı olarak erişilmesinin önlenmesi ve kişisel verilerin hukuka uygun saklanmasının sağlanması amacıyla kişisel veri işlenen tüm ortamlarda veri güvenliğini sağlamaya yönelik teknik ve idari tedbirlerin alınması konularında sorumlu birimlere aktif olarak destek verir.

Özel olarak, İnsan Kaynakları Birimi çalışanların politikaya uygun hareket etmesinden; Bilgi Teknolojileri Birimi Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından sorumlu olup, bahse konu her iki birim ayrıca Politika'nın geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesi açısından yetkili ve görevlidir.

VIII.Politika'ya Uyum

Tüm Şirket çalışanları, kişisel verilerin işlenmesi ve muhafazası sırasında Politika hükümlerine tam ve gereği gibi riayet etmekle mükellef olup, mezkûr politika çalışanların iş sözleşmelerinin ayrılmaz bir parçasını teşkil etmektedir.

Bu Politika'da yer alan hükümlerin ihlaline ilişkin somut emarelerin varlığı halinde Şirket yönetim organı şüphelenilen Politika ihlallerini araştırarak gerekli tedbirleri alır. İşbu politikaya uyulmaması, müşteri güven kaybı, dava, prestij kaybı, finansal kayıp ve Şirket itibarına zarar veya kişisel zarar dahil ve bunlarla sınırlı olmaksızın çeşitli olumsuz sonuçlara neden olabilir. Bu sebeple, bu politikaya herhangi bir şekilde uyulmaması Şirket çalışanları ya da ilgili sair kişiler hakkında disiplin soruşturması veya işin ya da sözleşmenin sona ermesi ile sonuçlanabilir. Anılan ihlal aynı zamanda dahil olan kişiler aleyhine hukuki işlemde bulunulmasına dahi yol açabilir.

IX. Yürürlük

Kişisel verilerin işlenmesi faaliyetlerinde yürürlükteki mevzuata tam uyumluluk hedefiyle tarafından hazırlanan işbu Politika, Gürok Turizm ve Madencilik Anonim Şirketi Yönetim Kurulu'nun … / … /2019 tarihli kararı ile onaylanarak yürürlüğe girmiştir.

Politika, basılı kağıt ve elektronik ortamda olmak üzere iki farklı ortamda yayınlanır. İç iletişime özgülenmiş elektronik ortamda çalışanlara açıklanır, basılı kâğıt nüshası da İnsan Kaynakları Departmanında saklanır. Politika, ihtiyaç hasıl oldukça gözden geçirilir ve gerektiğinde ilgili bölümler güncellenir.

Ek-1: Saklama ve İmha Süreleri Tablosu

İlgili Süreç ve Veri Kategorisi	Saklama Süresi	Açıklama
Çalışanlara ait kişisel sağlık verileri	İş ilişkisinin sona erme tarihinden itibaren 5 yıl	İş akdinin devamında ve hitamından itibaren olası meslek hastalığı/iş kazası tespit ve ihbarı ihtimaline karşılık 5 yıl süreyle saklanmaktadır.
Çalışanların işe alım dosyaları, özlük verileri	İş ilişkisinin sona erme tarihinden itibaren 20 yıl	Akdin kurulması için kullanılan veriler; olası bir hizmet/ücret tespiti talebi ile Sosyal Güvenlik Kurumu'nun alacak talebine istinaden hizmet akdinin devamınca ve hitamından itibaren 20 yıl süreyle muhafaza edilir.
Çalışan aday başvuru formları, özgeçmişleri	Başvuru tarihinden itibaren 1 yıl	En fazla 2 yıl olmak üzere özgeçmişin ve başvuru formlarının güncelliğini kaybedeceği süre kadar saklanır.
İş sağlığı ve güvenliği uygulamaları kapsamında elde edilen kişisel veriler	İş ilişkisinin sona erme tarihinden itibaren 15 yıl	İş akdinin taraflara yüklediği sorumluluklar kapsamında herhangi bir sağlık sorunu iddiasına karşılık iş ilişkisinin sona erme tarihinden itibaren 15 yıl süre ile saklanır.
Potansiyel müşteri bilgileri	Bilgilerin alındığı tarihten itibaren 2 yıl	Satış sözleşmesinin kurulabilmesi için aday müşterilerden elde edilen veriler 2 yıl müddetle muhafaza edilmektedir.
Müşteri talep ve şikayet yönetimi sırasında elde edilen veriler	İlk kaydın yapıldığı tarihten itibaren 1 yıl	Hizmetin devamını, kalitesini artırmak ve alıcının taleplerini değerlendirmek amacıyla alınan kişisel veriler ilk kaydın yapıldığı tarihten itibaren 1 yıl süre ile saklanmaktadır.
Finansal/Ödeme işlemlerine ait kayıtlar	İş ilişkisinin sona erme tarihinden itibaren 10 yıl	Akdin taraflara yüklediği yükümlülükler altında çalışanlara ücret ödemek için alınan veriler 10 yıl süre ile saklanmaktadır.
Gürok Turizm ve Madencilik Anonim Şirketi'nin işbirliği	İş akdi süresince ve bitiminden itibaren 10 yıl	İş akdi süresince aktarılan veriler ilgili iş süresince ve bitiminden itibaren sözleşme zamanaşımı olarak belirtilen

içinde olduğu firmalar/kurumlar ile paylaşılan bilgiler		10 yıl süre ile saklanmaktadır.
Alt yüklenici/ taşeron firma çalışanlarına ait kişisel veriler	İlgili sözleşmenin sona ermesinden itibaren 10 yıl	Şirket ile arasında yüklenici/taşeron ilişkisi olan firmaların çalışanlarına ait kişisel veriler sözleşme ilişkisi gereği 10 yıl süre ile muhafaza edilir.
Satış sözleşmesinin kapsamındaki kişisel veriler	İş ilişkisinin sona ermesinden itibaren 10 yıl	Sözleşmeden kaynaklı çıkabilecek uyuşmazlıklara karşılık sözleşme zamanaşımı süresince saklanmaktadır.
Üçüncü kişilerle imzalanan sözleşmeler kapsamındaki kişisel veriler	Sözleşmenin sona ermesinden itibaren 10 yıl	Sözleşme ilişkisi gereği 10 yıllık zamanaşımı süresince saklanmaktadır.
Güvenlik kamerası kayıtları	180 gün	İş yeri güvenliğini sağlamak amacıyla, şikâyet süresi de dikkate alınarak altı ay süreyle muhafaza edilir.
Ziyaretçi ve toplantı katılımcılarının kaydı	Etkinliğin sona ermesini takiben 2 yıl	Alınan veriler şirket içinde güvenlik sebebiyle meydana gelebilecek olumsuz durumlara karşı haksız fiil zamanaşımı olan 2 yıl süre ile muhafaza edilmektedir.
Çalışanlara araç tahsis edilmesi kapsamında elde edilen veriler	İş akdinin sona ermesini takiben 5 yıl	İş ilişkisinden doğan yükümlülükleri ifa etmek amacıyla çalışanlara araç tedarik edilmesi için alınan kişisel veriler, ücret alacaklarındaki zamanaşımı olan 5 yıl süre ile saklanmaktadır.
Kablosuz internet hizmet kullanımına ilişkin veriler	İlk kaydın yapıldığı tarihten itibaren 2 yıl	İnternet erişim hizmetinin sağlanması için elde edilen veriler yasa gereği 2 yıl süre ile saklanmaktadır.
Log kayıt takip sistemleri kapsamında tutulan veriler	Kaydın alındığı tarihten itibaren 2 yıl	İnternet erişim hizmetinin güvenli bir ortamda sağlanması amacıyla elde edilen kişisel veriler yasa gereği 2 yıl müddetle saklanmaktadır.
Gül Palas ve Ali Bey Hotels & Resorts misafirlerinden otel	Hizmet ilişkisinin sona ermesinden	Konaklama hizmeti çerçevesinde alınan kimlik bilgileri ve iletişim bilgileri, sözleşme zamanaşımı olan 10

rezervasyonu/kaydı için alınan bilgiler	itibaren 10 yıl	yıl müddetle muhafaza edilmektedir.
Gül Palas ve Ali Bey Hotels & Resorts misafirlerinden otel organizasyonları için alınan veriler	Hizmet ilişkisinin sona ermesinden itibaren 10 yıl	Sunulan hizmetler ile otel misafirlerinin taleplerini karşılamak amacıyla sözleşme kapsamında alınan veriler 10 yıl süre ile muhafaza edilmektedir.

Ek-2: Kişisel Veri İhlal Bildirimi Prosedürü

Kanunun 12 nci maddesinin (5) numaralı fıkrasının "*İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir….*" hükmünde yer alan "en kısa sürede" ifadesi 72 saat olarak yorumlanacaktır.

Bu kapsamda Gürok, söz konusu ihlali öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirecek, söz konusu veri ihlalinden etkilenen kişilerin Gürok tarafından belirlenmesini müteakip ilgili kişilere de makul olan en kısa süre içerisinde, ilgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa veri sorumlusunun kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılacaktır.

Gürok tarafından Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenleri de Kurula açıklanacaktır.

Kurula yapılacak bildirimde Kurul web sayfasında yer alan "Kişisel Veri İhlal Bildirim Form" kullanılacaktır. Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgiler gecikmeye mahal verilmeksizin aşamalı olarak Kurul'a sağlanacaktır.

Gürok tarafından veri ihlallerine ilişkin bilgiler, etkileri ve alınan önlemler kayıt altına alınacak ve Kurulun incelemesine hazır halde bulundurulacaktır.

Gürok adına veri işleyenler nezdinde bulunan kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyenin bu konuda herhangi bir gecikmeye yer vermeksizin Gürok'a bildirimde bulunmasına yönelik düzenlemeler yapılır.

Veri ihlali gerçekleşmesi halinde Bilgi Teknolojileri birimi, ihlalden etkilenen şirket birimlerini bilgilendirerek olası sonuçları ilişkin bir rapor hazırlar. Alınacak önlemler ve atılacak adımlara yönelik müdahale planı hazırlayarak eyleme geçirir.