ÖZEL İTALYAN ANA VE İLKOKULU
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI
6.11.2019 / Versiyon No: 1

İÇİNDEKİLER

ÖZEL İTALYAN ANA VE İLKOKULU
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI
6.11.2019 / Versiyon No: 1

1. Amaç

1.1. Bu Kişisel Veri Saklama ve İmha Politikası (Politika) "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in" 5. maddesi çerçevesinde veri sorumlusunun (Şirket) kişisel veri işleme envanterine uygun olarak hazırlanmıştır.

1.2. Bu Politika Şirket'in tabi olduğu kanun ve ikincil mevzuata uyumu sağlayabilmek adına Şirket'in kişisel veri saklama ve imhaya ilişkin ilkelerini belirlemektedir.

1.3. Bu Politika, Şirket tarafından gerçekleştirilmekte olan saklama ve imha faaliyetlerine ilişkin yapılması gerekenler hakkında usul ve esasları belirlemek amacıyla hazırlanmıştır.

1.4. Bu Politika, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda (Kanun) belirlenen aşağıdaki ilkeleri gözetmektedir. Kanun uyarınca kişisel verilerin işlenmesinin;

- Hukuka ve dürüstlük kurallarına uygun olması;
- Doğru ve gerektiğinde güncel olması;
- Belirli, açık ve meşru amaçlar için işlenmesi;
- İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması;
- İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerekmektedir.

1.5. Bu Politika, Şirket'in faaliyetleri çerçevesinde düzenlenmiş, asılları ve kopyaları dahil tüm fiziksel ve elektronik belgelere/ortamlara uygulanır.

1.6. Yürürlükteki mevzuat Şirket'in belli kayıtları, belli sürelerle saklamasını gerektirebilir. Bu saklama sürelerine uymamak Şirket'i cezalara ve yaptırımlara maruz bırakabilir, adaletin yerine getirilmesini engelleyebilir, yasal delillerin delil özelliklerini yitirmesine neden olabilir ve/veya hukuki süreçlerde Şirket'in konumunu önemli ölçüde zedeleyebilir. Bu yüzden Politika;

1.6.1. Yürürlükteki mevzuat kapsamında hazırlanan ve süreçler ile spesifik saklama sürelerini belirleyen bir "EK-A / Saklama ve İmha Süreleri Tablosunu" içermektedir.

1.6.2. Ayrıca, Veri Sorumlusu nezdinde saklama ve imha süreçleriyle Şirket içinde hangi kişilerin/birimlerin ilgili ve sorumlu olduğu ile bu kişilerin/birimlerin görevlerini belirleyen bir "EK-B / Saklama ve İmha Sürecinde Yer Alan Kişiler Tablosu" Politika içinde yer almaktadır.

1.7. Şirket çalışanları bu Politika'yı tam olarak anlamak ve uygulamakla yükümlüdür.

2. Tanımlar

Özel isim olmadıkça ve Politika içerisinde ayrı bir yerde tanımlanmadıkça, aşağıda listelenen terimler, tanımlandıkları anlamlara gelirler:

Açık Rıza	Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı ifade eder.
Alıcı Grubu	Veri Sorumlusu tarafından kişisel verilerin aktarıldığı gerçek veya tüzel kişi kategorisini ifade eder.

Aktif Kayıtlar	Şirket'in işleyişi, idaresi ve yönetimi için halen kullanılmakta olan kayıtları ifade eder.
Aktif Olmayan Kayıtlar	Kullanılmayan; ancak işlenmesi sonradan gerekebileceği için saklama süreleri sona ermemiş kayıtları ifade eder.
Anonim Hale Getirme	Kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini ifade eder.
Çalışan	Veri sorumlusu bünyesinde çalışan gerçek kişileri ifade eder.
De-manyetize Etme	Manyetik medyanın özel bir cihazdan geçirilerek gayet yüksek değerde bir manyetik alana maruz bırakılması ile üzerindeki verilerin okunamaz biçimde bozulması işlemini ifade eder.
Elektronik Ortam	Elektronik ortam, insan müdahalesi ihtiyacını asgari seviyeye indirilerek verilerin tutulduğu, mantıksal veya aritmetik işlemlerin uygulandığı, verilerin değiştirilmesi, silinmesi, geri elde edilmesi veya aktarılması gibi işlemlerin otomatik veya kısmen otomatik yöntemlerle gerçekleştirildiği ortamları ifade eder.
Elektronik Olmayan Ortam	Bir veri kayıt sistemine bağlı olarak otomatik olmayan yollarla işleme ise manuel olarak hazırlanan ancak erişimi ve anlamlandırmayı kolaylaştıran işleme faaliyetini ifade eder.
Fiziksel Yok Etme (*Elektronik Veriler İçin*)	Optik medya ve manyetik medyanın eritilmesi, yakılması veya toz haline getirilmesi gibi fiziksel olarak yok edilmesini ifade eder.
Hizmet Sağlayıcılar	Veri Sorumlusu'na ürün veya hizmet satmak amacıyla ticari faaliyette bulunan gerçek ve tüzel kişiler ile bu hizmetlere aracılık eden gerçek ve tüzel kişileri ifade eder.
İki Kademeli Kimlik Doğrulama	Kişinin kullanıcı adı ve şifresi ile, dışarıdan ayrı bir kimlik doğrulama sisteminin (cep telefonu, kişisel soru, kriptografik anahtar vb.) birleşiminden oluşan doğrulama sistemini ifade eder.
İkincil Mevzuat	Kanun uyarınca, Kişisel Verileri Koruma Kurumu tarafından çıkarılan ya da alınan herhangi bir yönetmelik, genelge, tebliğ, ilke kararı veya benzeri bir idari karar ya da genel görüş anlamına gelir.
İlgili Kişi	Kişisel verisi işlenen gerçek kişiyi ifade eder.
İlgili Kullanıcılar	Verilerin teknik olarak depolanması, korunması ve yedeklenmesinden sorumlu olan kişi ya da birim hariç olmak üzere Veri Sorumlusu

	organizasyonu içerisinde veya Veri Sorumlusu'ndan aldığı yetki ve talimat doğrultusunda kişisel verileri işleyen kişileri ifade eder.
İmha	Silme, yok etme ve/veya anonim hale getirme işlemlerinden herhangi birini veya tümünü ifade eder.
Kanun	6698 sayılı Kişisel Verileri Koruma Kanunu'nu ifade eder.
Karartma/Maskeleme	Kişisel verilerin bütününün, kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek şekilde üstlerinin çizilmesi, boyanması, buzlanması, yıldızlanması gibi işlemleri ifade eder.
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 ifade eder.
Kişisel Veri	Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder.
Kayıtlı Elektronik Posta (KEP)	Elektronik iletilerin, gönderimi ve teslimatı da dahil olmak üzere kullanımına ilişkin olarak hukuki delil sağlayan, elektronik postanın nitelikli şeklini ifade eder.
Kişisel Veri İşleme Envanteri	Veri Sorumlusu'nun iş süreçlerine bağlı olarak gerçekleştirmekte olduğu kişisel verileri işleme faaliyetlerini; kişisel verileri işleme amaçlarını, hukuki sebeplerini, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturduğu ve kişisel verilerin işlendikleri amaçlar için gerekli olan muhafaza edilme sürelerini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri detaylandıran envanteri ifade eder.
Kurul	Kişisel Verileri Koruma Kurulu'nu ifade eder.
Kurum	Kişisel Verileri Koruma Kurumu'nu ifade eder.
KVK Danışma Grubu	Şirket içerisinde Kanun'a uyumlulaştırma projesinin tamamlanması ve sonrasındaki danışmanlık hizmetlerini yürüten şirket çalışanlarını ifade eder.
Özel Nitelikli 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 ifade eder.

Periyodik İmha	Kanun'da yer alan kişisel verilerin işlenme şartlarının tamamının ortadan kalkması durumunda Kişisel Verileri Saklama Ve İmha Politikası'nda belirtilen ve tekrar eden aralıklarla resen gerçekleştirilecek silme, yok etme veya anonim hale getirme işlemini ifade eder.
Politika	Bu Kişisel Veri Saklama ve İmha Politikası'nı ifade eder.
Saklama ve İmha Süreleri Tablosu	Ek A'da yer alan "Saklama ve İmha Süreleri Tablosunu" ifade eder.
SFTP	Kriptografik ağ protokolü SSH kullanarak dosya transferi yapan bir dosya aktarım protokolüdür.
Silme	Kişisel verilerin İlgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemini ifade eder.
Şirket	Veri Sorumlusu'nu ifade eder.
Üzerine Yazma	Manyetik medya ve yeniden yazılabilir optik medya üzerine en az yedi kez 0 ve 1'lerden oluşan rastgele veriler yazarak eski verinin kurtarılmasının önüne geçilmesi işlemini ifade eder.
VERBİS	Veri Sorumluları Sicili (VERBİS), veri sorumlularının kayıt olmak zorunda oldukları ve veri işleme faaliyetleri ile ilgili bilgileri beyan ettikleri bir kayıt sistemidir.
Veri İşleyen	Veri Sorumlusu'nun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade eder.
Veri Kayıt Sistemi	Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini ifade eder.
Veri Sorumlusu	Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, Veri Kayıt Sistemi'nin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade eder.
Veri Sorumlusu İrtibat Kişisi	Türkiye'de yerleşik olan gerçek ve tüzel kişiler için veri sorumlusu tarafından, Türkiye'de yerleşik olmayan gerçek ve tüzel kişiler için de veri sorumlusu temsilcisi tarafından, Kanun ve bu Kanun'a dayalı olarak çıkarılacak ikincil düzenlemeler kapsamındaki yükümlülükleriyle ilgili olarak, Kurum ile iletişimi sağlamak amacıyla sicile kayıt esnasında bildirilen gerçek kişiyi ifade eder.

Veri Yetkilisi	Veri Sorumlusu tarafından atanan ve Kanun'a uygun olarak Şirket kişisel veri envanterini oluşturan, güncel tutan ve gerekli değişiklikleri Veri Sorumlusu İrtibat Kişisine ileten şirket çalışanını ifade eder.
Yok Etme	Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemi ifade eder.
Yönetmelik	28 Ekim 2017 tarihinde Resmi Gazete'de yayımlanan ve 1 Ocak 2018 tarihinde yürürlüğe giren Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'i ifade eder.

Burada yer almayan tanımların, Kanun ve ikincil düzenlemelerde belirtilen anlamları ile kullanıldığı kabul edilecektir.

3. Kapsam

3.1. Bu Politika, Şirket'in tamamına uygulanır ve gerekli yükümlülükleri düzenler. Şirket tarafından kişisel verileri işlenen tüm gerçek kişilere ilişkin kişisel veriler bu Politika kapsamındadır. Şirket'in sahip olduğu ya da Şirket tarafından yönetilen kişisel verilerin işlendiği tüm kayıt ortamları hakkında ve tüm veri işleme faaliyetlerinde bu Politika uygulanacaktır.

3.2. Şirket, Veri Sorumlusu olarak kişisel veri işlediğinde, bu Politika'da yer alan düzenlemelere uygun davranır.

3.3. Şirket, bir başkası namına Veri İşleyen olarak kişisel veri işlediği durumda bu Politika'da yer alan düzenlemelere ve varsa, söz konusu üçüncü kişi ile imzalanan her türden sözleşmedeki, Politika'ya aykırı olmayan, talimatlara uyar.

3.4. Politika'nın uygulanmasından ve Politika'ya uyumun sağlanmasından ilgili departman yöneticisi, Veri Sorumlusu İrtibat Kişisi ve Veri Yetkilisi sorumludur.

4. Kişisel Verilerin Saklanmasını ve İmhasını Gerektiren Nedenler

4.1. Şirketimiz;

- 213 Sayılı Vergi Usul Kanun'u,
- 2004 Sayılı İcra İflas Kanun'u,
- 4857 Sayılı İş Kanun'u,
- 5237 Sayılı Türk Ceza Kanun'u,
- 5510 Sayılı SSGSK Kanun'u,
- 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun,
- 6201 Sayılı Türk Ticaret Kanun'u,
- 6098 Sayılı Borçlar Kanun'u,
- 6331 Sayılı İş Sağlığı ve Güvenliği Kanun'u,
- 6698 Sayılı Kişisel Verilerin Korunması Kanun'u, ilgili yönetmelikleri gereği ve bunlarla sınırlı olmamak üzere yayınlanan diğer mevzuat hükümleri,

- Çalışma Bakanlığı ve SGK müfettişlerince yapılan denetimlerde,
- İstatistiksel çalışmalar için,
- Ayrıca mahkeme ve bilirkişi incelemelerinde sunmak üzere,
- Yerel kolluk kuvvetleri ve organize sanayi müdürlüklerince istenmesi durumunda,

kişisel veriler işlenebilir, saklamak ve gereği geldiğinde silmek üzere kayıt altına alınabilir.

4.2. Kişisel verilerin saklanmasını gerektiren işleme amaçları; insan kaynakları süreçlerini yürütmek, kurumsal iletişimi sağlamak, şirket güvenliğini sağlamak, istatistiksel çalışmalar yapabilmek, imzalanan sözleşmeler ve protokoller neticesinde iş ve işlemleri ifa edebilmek, yasal düzenlemelerin gerektirdiği veya zorunlu kıldığı şekilde, hukuki yükümlülüklerin yerine getirilmesini sağlamak, şirket ile iş ilişkisinde bulunan gerçek / tüzel kişilerle irtibat sağlamak, iş sağlığı güvenliği süreçlerinin yürütülmesini sağlamak, bilgi sistemleri süreçlerini yürütmek, ziyaretçi, kamera ve toplantı kayıtlarını tutmak, müşteri verilerini işlemek, tedarik süreçlerini yönetmek, muhasebe ve finans süreçlerini yürütmek, seyahat süreçlerini takip etmek, posta, kargo, gönderi kayıtlarını işlemek tır.

5. Kayıt Ortamları

5.1. Fiziksel Kayıtlar

5.1.1. Yazılı, basılı ortamlar ve manuel veri kayıt sistemleri (anket formları, ziyaretçi giriş defteri) gibi fiziksel ortamlar, fiziksel kayıtlar, kağıt üzerindeki kayıtlar, fotoğraflar ve sözleşmeler gibi kağıt, mikro fiş ve benzeri ortamlarda bulunan kayıtlardan oluşur.

5.1.2. Aktif kayıtlar ve kolayca erişilmesi gereken kayıtlar Şirket'in ofis ortamında depolanabilir.

5.1.3. Aktif olmayan kayıtlar Şirket'in arşivlerine gönderilir.

5.2. Elektronik Kayıtlar

5.2.1. Ses kayıtları, fotoğraflar, videolar ve görsel ve işitsel ortamlar dahil birçok ortamda yer alan kişisel veriler; doğru, güncel ve kişisel verileri işlemesi gereken kişilerce erişilebilir olacak şekilde, yetkisiz üçüncü kişilerce erişimi ve işlemeyi engelleyecek düzeyde güvenli elektronik ortamlarda saklanabilir. Elektronik ortamlara örnek olarak;

- Sunucular (Etki alanı, yedekleme, e-posta, veri tabanı, web, dosya paylaşım vb.),
- Yazılımlar (ofis yazılımları, portal vb.),
- Bilgi güvenliği cihazları (güvenlik duvarı, saldırı tespit, engelleme, günlük kayıt dosyası, anti virüs vb.),
- Yedekleme kartuşları,
- Kişisel bilgisayarlar (Masaüstü, dizüstü),
- Mobil cihazlar (telefon, tablet vb.),
- Optik diskler (CD, DVD vb.),
- Çıkartılabilir bellekler (USB, hafıza kartı vb.),
- Yazıcı, tarayıcı, fotokopi makinesi vb. diğer elektronik veri kayıt ortamları sayılabilir.

5.2.2. Elektronik kayıtların, kaybedilmeye, değiştirilmeye ve izinsiz yok edilmeye, saklanma süreçlerinde erişime karşı korunmalarını sağlamak ve eksiksiz, doğru ve okunaklı olmasını temin etmek için yeterli koruma önlemleri alınmalı, süreçler oluşturulmalı ve Şirket tarafından uygulanmalıdır.

6. Saklama ve İmha Süreleri, Periyodik İmha

6.1. EK-A spesifik süreçlerle birlikte bunların saklama sürelerini içermektedir. EK-B bu süreçlerde kimlerin yer aldığını ve bu kişilerin/birimlerin görevlerini içermektedir.

6.2. Bu Politika bağlamında, saklama takvimi kaydın oluşturulduğu takvim yılının sonunda başlar. Saklama süresi dolmuş tüm kayıtlar yılda iki kez imha edilir. İlk periyodik imha takvim yılının sonunda, ikinci ise her yıl Haziran ayının sonunda yapılır ve Periyodik İmhalar arasında süre her halde altı ayı geçemez. Bir kişisel verinin işleme amacının ortadan kalktığı tarih bu iki dönemden hangisine daha yakınsa o dönemde İmha edilir. (Örneğin; bir kayıt Mart 2010'da oluşturulduysa ve yedi yıl boyunca tutulması gerekiyorsa, Kayıt 30 Haziran 2017 tarihinde İmha edilir; eğer söz konusu kayıt Kasım 2010'da oluşturulmuş olsaydı 31 Aralık 2017 tarihinde İmha edilmesi gerekecekti.)

7. İmha

7.1. Kayıtlar, aşağıdaki hallerde imha edilmelidir.

7.1.1. Kişisel verilerin aşağıdaki koşullardan hangisinin gerçekleşmesi halinde silineceği ve bu koşulların gerçekleşmesi halinde alınacak aksiyonlar, somut olayın koşullarına, Kanun, Yönetmelik ve İkincil Mevzuat hükümlerine göre Üst Yönetim, Veri Sorumlusu İrtibat Kişisi ve KVK Danışma Grubu tarafından belirlenir ve şirket veri envanterlerinde güncel haliyle, saklama süreleri de belirtilerek, kayıt altına alınır.

- Kişisel verileri işleme şartlarının tamamının ortadan kalkması koşuluyla İlgili Kişi, kişisel verisinin imhasını talep ettiğinde,
- İlgili Kişi, kişisel verisinin işlenmesi ile ilgili açık rızasını geri aldığında,
- Kişisel verilerin işlenmesine veya saklanmasına ilişkin gereklilikler ve/veya amaçlar ortadan kalktığında,
- Kişisel verilerin işlenmesine esas teşkil eden ilgili mevzuat hükümlerinin değiştirilmesi veya ilgası halinde,
- Kurum, usulüne uygun olarak kişisel verinin imhasını talep ettiğinde,
- Kişisel verinin saklama süresi sona erdiğinde imha edilir.

7.1.2. Kişisel verileri işleme şartlarının tamamının ortadan kalkmaması halinde İlgili Kişi'nin kişisel verisinin imhasını talep etmesi durumunda bu talep, Veri Sorumlusu İrtibat Kişisi tarafından hazırlanacak yazılı gerekçe ile reddedilebilir. Bu yazılı gerekçe şirkete, talebin tebliğ edildiği tarihten itibaren 30 (otuz) gün içerisinde talepte bulunan İlgili Kişi'ye gönderilir. Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa, talebe konu Kişisel Veriler imha edilir. Bu bağlamda İlgili Kişi'nin talebi tebliğ edildiği tarihten itibaren en geç 30 (otuz) gün içerisinde sonuçlandırılır ve İlgili Kişi'ye bilgi verilir.

7.1.3. Şirket, Veri Sorumlusu İrtibat Kişisi ve KVK Danışma Grubu aracılığı ile imha yöntemlerinden uygun olanı seçer. İlgili kişinin talebi durumunda ise, uygun yöntemi seçmesinin gerekçesini açıklar. Bu gerekçenin açıklaması Veri Sorumlusu İrtibat Kişisi tarafından yapılır ve İlgili Kişi'nin talebi halinde, Kanun, Yönetmelik ve ikincil mevzuata uygun şekilde İlgili Kişi'ye iletilir.

7.1.4. Kişisel Verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişiye aktarılmışsa bu durum üçüncü kişiye bildirilir ve üçüncü kişi nezdinde Yönetmelik kapsamında imha ile ilgili gerekli işlemlerin yapılması takip edilir.

7.2. Kayıtların Yok Edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi ile sağlanır. Kişisel verilerin yok edilmesi için, verilerin bulunduğu tüm kopyaların tespit edilmesi ve verilerin hiçbir şekilde erişilememesini, geri getirilememesini ve tekrar kullanılamamasını sağlamak gerekir. Kişisel verilerin yok edilmesi faaliyeti, Veri Sorumlusu İrtibat Kişisi tarafından imzalanmış yok etme kararını aldıktan sonra, Şirket tarafından yerine getirilir. Veri Sorumlusu İrtibat Kişisi, yok etme faaliyetinden sorumlu kişileri, neden ilgili yok etmenin gerekli olduğu konusunda bilgilendirir.

7.2.1. Elektronik Kayıtlar;

- Elektronik kayıtlar de-manyetize etme, fiziksel yok etme ve üzerine yazma yollarıyla yok edilebilir.
- Ağ cihazlarının (switch, router vb.) içindeki saklama ortamları sabittir. Ürünler, çoğu zaman silme komutuna sahiptir ama veriyi yok etme özelliği bulunmamaktadır. De-manyetize etme, fiziksel yok etme, üzerine yazma yöntemlerin bir ya da birkaçı kullanılmak suretiyle veri yok edilir.
- Kişisel verilerin yer aldığı flash tabanlı sabit disklerin ATA (SATA, PATA vb.), SCSI (SCSI Express vb.) arayüzüne sahip olanları için, destekleniyorsa yok etme komutunu kullanmak, desteklenmiyorsa üreticinin önerdiği yok etme yöntemini kullanmak ya da de-manyetize etme, fiziksel yok etme, üzerine yazma yöntemlerin bir ya da birkaçı kullanılmak suretiyle yok edilir.
- Taşınabilir akıllı telefonlardaki sabit hafıza alanlarında silme komutu bulunmakta, ancak çoğunda yok etme komutu bulunmamaktadır. De-manyetize etme, fiziksel yok etme, üzerine yazma yöntemlerin bir ya da birkaçı kullanılmak suretiyle veri yok edilir.
- CD, DVD gibi veri saklama ortamlarında yer alan kişisel veriler, yakma, küçük parçalara ayırma, eritme gibi fiziksel yok etme yöntemleriyle yok edilir.
- Kayıt ortamı çıkartılabilir olan yazıcı, parmak izli kapı geçiş sistemi gibi çevre birimlerinde yer alan kişisel veriler için, tüm kayıt ortamlarının söküldüğü doğrulandıktan sonra birimin niteliğine göre uygun yok etme yöntemi seçilir.

7.2.2. *Fiziksel kayıtlar* ise kağıt imha veya kırpma makinaları ile anlaşılmaz boyutta (mümkünse dikey ve yatay şekilde parçalanarak) veya okunmasını imkânsız kılacak başka yöntemlerle (örneğin, kaydı birleştirilemeyecek ufak parçalara kesmek veya fiziksel kaydı uygun bir ortamda yakmak vb.) İmha edilir.

7.2.3. *Bulut sistemleri* için; bu sistemlerde yer alan kişisel verilerin depolanması için kullanılan veri tabanları kriptografik yöntemlerle şifrelenir ve kişisel veriler için mümkün olan yerlerde, özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılır. Bulut bilişim hizmet ilişkisi sona erdiğinde; kişisel verileri kullanılır hale getirmek için gerekli şifreleme anahtarlarının tüm kopyaları yok edilir.

Commented [AA1]: Arkas Bilgi Sistemleri Direktörlüğü (BSD) şemsiyesi dışında kalan iştiraklerin irtibat kişileri 7.2, 7.3, ve 7.4 maddelerinde tarif edilen yöntemleri kendi güncel uygulamalarına göre gözden geçirmelidir.
Eğer burada listelenen yöntemler içinde teknik olarak uygulanamayacak yöntemler var ise, bunlar ilgili iştirakin politika metninden çıkarılmalıdır.

7.2.4. *Arızalanan ya da bakıma gönderilen cihazlar* için; bu cihazlarda yer alan kişisel verilerin yok edilmesi işlemleri ise aşağıdaki şekilde gerçekleştirilir:

- İlgili cihazların bakım, onarım işlemi için üretici, satıcı, servis gibi üçüncü kurumlara aktarılmadan önce içinde yer alan kişisel verilerin Şirket tarafından uygun görülen yöntemle yok edilmesi,
- Yok etmenin mümkün ya da uygun olmadığı durumlarda, veri saklama ortamının sökülerek saklanması, arızalı diğer parçaların üretici, satıcı, servis gibi üçüncü kurumlara gönderilmesi,
- Dışarıdan bakım, onarım gibi amaçlarla gelen personelin, kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınması,

Çalışanlar, kaydın nasıl yok edileceğine ve yukarıda belirtilen yok etme yöntemlerine dair Veri Sorumlusu İrtibat Kişisinden tavsiye alabilirler.

7.3. Silme İşlemi

7.3.1. Kişisel verilerin İlgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi ile gerçekleştirilir. Kişisel verilerin silinmesi işleminde izlenmesi gereken süreç aşağıdaki gibidir:

- Silme işlemine konu teşkil edecek kişisel verilerin belirlenmesi,
- Erişim yetki ve kontrol matrisi ya da benzer bir sistem kullanarak her bir kişisel veri için İlgili 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.

7.3.2. *Bulut sunucu kullanan uygulamaların (Office 365 vb.) sunucularında yer alan kişisel veriler:* sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır.

7.3.3. *Fiziksel kayıtlarda yer alan kişisel veriler:* Fiziksel ortamda tutulan kişisel veriler arasında saklama süresi sona eren dokümanlar, evrak arşivinden sorumlu birim yöneticisi tarafından imha edilir veya hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilir.

7.3.4. *Şirket sunucularında yer alan kişisel veriler*: Sunucularda yer alan kişisel verilerden saklanmasını gerektiren süre sona erenler için sistem yöneticisi tarafından ilgili kullanıcıların erişim yetkisi kaldırılarak silme işlemi yapılır. Anılan işlem gerçekleştirilirken, ilgili kullanıcı aynı zamanda sistem yöneticisi ise, ilgili kişinin sistem yöneticisi yetkilerinin kaldırılması veya başka bir imha yöntemi gerçekleştirilmesi gerekir.

7.3.5. *Flash disk, harici HDD gibi taşınabilir medya ortamlarında yer alan kişisel veriler*, şifreli olarak saklanır ve erişim yetkisi sadece sistem yöneticisine verilerek şifreleme anahtarlarıyla güvenli ortamlarda saklanır.

7.3.6. *Veri tabanlarında bulunan kişisel veriler*, kişisel verilerin bulunduğu ilgili satırların veri tabanı komutları ile ("delete" vb.) silinmesi suretiyle silinir. Anılan işlem gerçekleştirilirken ilgili kullanıcı aynı zamanda veri tabanı yöneticisi ise ilgili kişinin veri tabanı yöneticisi yetkilerinin

kaldırılması veya başka bir imha yöntemi gerçekleştirilmesi gerekir.

7.4. Anonim Hale Getirme

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

Bu özelliklerin engellenmesi veya kaybedilmesi sonucunda belli bir kişiye işaret etmeyen veriler, anonim hale getirilmiş veri sayılır. Diğer bir ifadeyle anonim hale getirilmiş veriler bu işlem yapılmadan önce gerçek bir kişiyi tespit eden bilgiyken bu işlemden sonra ilgili kişi ile ilişkilendirilemeyecek hale gelmiştir ve kişiyle bağlantısı kopartılmıştır.

Anonim hale getirmedeki amaç, veri ile bu verinin tanımladığı kişi arasındaki bağın kopartılmasıdır. Kişisel verinin tutulduğu veri kayıt sistemindeki kayıtlara uygulanan otomatik olan veya olmayan gruplama, maskeleme, türetme, genelleştirme, rastgele hale getirme gibi yöntemlerle yürütülen bağ koparma işlemlerinin uygulanması sonucunda elde edilen veriler, belirli bir kişiyi tanımlayamaz hale getirdiğinde anonim hale getirme gerçekleşmiş sayılır.

Kullanılabilecek anonim hale getirme yöntemlerinden bazıları örnek olarak aşağıda sıralanmıştır:

7.4.2. 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. Değer düzensizliği sağlamayan anonim hale getirme yöntemlerinden bazıları aşağıda örneklerle açıklanmıştır:

7.4.2.1. *Değişkenleri çıkartma :* Değişkenlerden birinin veya birkaçının tablodan bütünüyle silinerek çıkartılmasıyla sağlanan bir anonim hale getirme yöntemidir. böyle bir durumda tablodaki bütün sütun tamamıyla kaldırılacaktır. Bu yöntem, değişkenin yüksek dereceli bir tanımlayıcı olması, daha uygun bir çözümün var olmaması, değişkenin kamuya ifşa edilemeyecek kadar hassas bir veri olması veya analitik amaçlara hizmet etmiyor olması gibi sebeplerle kullanılabilir. Örneğin; kişilerin yaş, cinsiyet, posta kodu, gelir, din verilerinin yer aldığı bir tablodan "din" sütunun tamamen çıkartılması.

7.4.2.2. *Kayıtları Çıkartma :* Bu yöntemde ise veri kümesinde yer alan tekillik ihtiva eden bir satırın çıkartılması ile anonim olma durumu kuvvetlendirilir ve veri kümesine dair varsayımlar üretebilme ihtimali düşürülür. Genellikle çıkartılan kayıtlar diğer kayıtlarla ortak bir değer taşımayan ve veri kümesine dair fikri olan kişilerin kolayca tahmin yürütebileceği kayıtlardır. Örneğin; anket sonuçlarının yer aldığı bir veri kümesinde, herhangi bir sektörden yalnızca tek bir kişi ankete dahil edildiyse, böyle bir durumda tüm anket sonuçlarından "sektör" değişkenini çıkartmaktansa sadece bu kişiye ait kaydın çıkartılması.

7.4.2.3. *Bölgesel Gizleme :* Bölgesel gizleme yönteminde de amaç veri kümesini daha güvenli hale getirmek ve tahmin edilebilirlik riskini azaltmaktır. Belli bir kayda ait değerlerin yarattığı

kombinasyon çok az görülebilir bir durum yaratıyorsa ve bu durum o kişinin ilgili toplulukta ayırt edilebilir hale gelmesine yüksek olasılıkla sebep olabilecekse istisnai durumu yaratan değer "bilinmiyor" olarak değiştirilir. Örneğin; bir tabloda yaş, cinsiyet ve meslek ayrımına göre hastalık durumunun belirtildiği düşünüldüğüne, bu tabloda yaş=3 olan kayıt bir çocuğa ait olduğundan istisnai bir durum yaratmakta ve tahmin edilebilirlik ve çocuğun ailesine dair varsayımlar yapılması riskini arttırmaktadır. Bu sebeple; bölgesel gizleme yöntemi ile bahsedilen kaydın yaş hanesi "bilinmiyor" olarak değiştirilirse, veri kümesine dair tahmin edilebilirlik riskinde azalma sağlanacaktır.

7.4.2.4. *Genelleştirme :* İlgili kişisel veriyi özel bir değerden daha genel bir değere çevirme işlemidir. Kümülatif raporlar üretirken ve toplam rakamlar üzerinden yürütülen operasyonlarda en çok kullanılan yöntemdir. Sonuç olarak elde edilen yeni değerler gerçek bir kişiye erişmeyi imkânsız hale getiren bir gruba ait toplam değerler veya istatistikleri gösterir. Örneğin; TC kimlik numarası 12345678901 olan bir kişi e-ticaret platformundan bir ürün aldıktan sonra aynı zamanda başka bir ilişkili ürün de aldıysa, yapılacak anonim hale getirme işleminde genelleştirme yöntemi kullanılarak e-ticaret platformundan ilk ürünü kişilerin %xx'i aynı zamanda ikinci ürünü de satın alıyor şeklinde bir sonuca ulaşılabilir.

7.4.2.5. *Alt ve Üst Sınır Kodlama :* Alt ve üst sınır kodlama yöntemi belli bir değişken için bir kategori tanımlayarak bu kategorinin yarattığı gruplama içinde kalan değerleri birleştirerek elde edilir. Genellikle belli bir değişkendeki değerlerin düşük veya yüksek olanları bir araya toplanır ve bu değerlere yeni bir tanımlama yapılarak ilerlenir. Örneğin; kişilerin yıllık gelirlerinin yer aldığı bir tabloda yıllık gelirlerin birebir yansıtılması yerine, alt sınırı 100.000, üst sınırı 120.000 alarak tabloda; 100.000 TL'den küçük ve eşit değerler, "düşük", 100.000 ve 120.000 arası değerler "orta", 120.000'den büyük ve eşit değerler "yüksek" olarak gruplandırılabilir.

7.4.2.6. *Global Kodlama:* Global kodlama yöntemi alt ve üst sınır kodlamanın uygulanması mümkün olmayan, sayısal değerler içermeyen veya sayısal olarak sıralanamayan değerlere sahip veri kümelerinde kullanılan bir gruplama yöntemidir. Genelde belli değerlerin öbeklenerek tahmin ve varsayımlar yürütmeyi kolaylaştırdığı hallerde kullanılır. Seçilen değerler için ortak ve yeni bir grup oluşturularak veri kümesindeki tüm Kayıtlar bu yeni tanım ile değiştirilir. Örneğin; bir veri kümesinde tek bir birimdeki kadınların sayısına ait verinin meslek değişkeninde iki kategoride yığılma varsa (mesela o kümedeki kadınların çoğunluğu mimar veya mühendis ise) söz konusu iki kategorinin birleşiminden tek bir kategori elde edilebilir (ayrı ayrı "mimar" ve "mühendis" kategorileri yerine "mimar veya mühendis" adlı bir kategori üretilebilir).

7.4.2.7. *Örnekleme* : Örnekleme yönteminde bütün veri kümesi yerine, kümeden alınan bir alt küme açıklanır veya paylaşılır. Böylelikle bütün veri kümesinin içinde yer aldığı bilinen bir kişinin açıklanan ya da paylaşılan örnek alt küme içinde yer alıp almadığı bilinmediği için kişilere dair isabetli tahmin üretme riski düşürülmüş olur. Örnekleme yapılacak alt kümenin belirlenmesinde basit istatistik metotları kullanılır. Örneğin; İstanbul ilinde yaşayan insanların demografik bilgileri, meslekleri ve sağlık durumlarına dair bir veri kümesini anonim hale getirerek açıklanması ya da paylaşılması halinde İstanbul'da yaşadığı bilinen bir insana dair ilgili veri kümesinde taramalar yapmak ve tahmin yürütmek anlamlı olabilir. Ancak ilgili veri

kümesinde yalnızca nüfusa kayıtlı olduğu il İstanbul olan insanların kayıtları bırakılır ve nüfus kaydı diğer illerde olanlar veri kümesinden çıkartılarak anonimleştirme uygulanır ve veri açıklanır ya da paylaşılırsa, veriye erişen kötü niyetli kişi İstanbul'da yaşadığını bildiği bir insanın nüfus kaydının İstanbul'da olup olmadığını tahmin edemeyeceğinden tanıdığı bu kişiye ait bilgilerin elindeki verinin içerisinde yer alıp almadığına dair güvenilir bir tahmin yürütemeyecektir.

7.4.3. Değer Düzensizliği Sağlayan Anonim Hale Getirme Yöntemleri

7.4.3.1. *Mikro-Birleştirme* : Bu yöntem ile veri kümesindeki bütün kayıtlar öncelikle anlamlı bir sıraya göre dizilip sonrasında bütün küme belirli bir sayıda alt kümelere ayrılır. Daha sonra her alt kümenin belirlenen değişkene ait değerinin ortalaması alınarak alt kümenin o değişkenine ait değeri ortalama değer ile değiştirilir. Böylece o değişkenin tüm veri kümesi için geçerli olan ortalama değeri de değişmeyecektir. Örneğin; bir tablodaki "Gelir" sütununda "25.000, 28.000, 37.000, 49.000, 56.000 ve 60.000" değerlerinin olduğu varsayıldığında ilk üç değer (25.000, 28.000, 37.000) "Grup 1", sonraki üç değer (49.000, 56.000 ve 60.000) "Grup 2" olarak ayırılır. Sonrasında Grup 1'de yer alan değerlerin ortalaması alınır ([25.000 + 28.000 + 37.000] / 3 = 30.000) ve Grup 1 için bütün gelir değerlerine, kendi değerleri yerine 30.000 yazılır. Aynı işlem Grup 2 için de yapılır.

7.4.3.2. *Veri Değiş-Tokuşu* : Veri değiş tokuşu yöntemi, kayıtlar içinden seçilen çiftlerin arasındaki bir değişken alt kümeye ait değerlerin değiş tokuş edilmesiyle elde edilen kayıt değişiklikleridir. Bu yöntem temel olarak kategorize edilebilen değişkenler için kullanılmaktadır ve ana fikir değişkenlerin değerlerini bireylere ait Kayıtlar arasında değiştirerek veri tabanının dönüştürülmesidir. Örneğin; Yaş, Cinsiyet, İl ve Gelir değerlerini gösteren bir tabloda, Yaş="24", Cinsiyet="K", İl="Ankara" olan kayda ait gelir bilgisi ile Yaş="45", Cinsiyet="E", İl="İzmir" olan kaydın gelir bilgisi birbirleriyle değiştirilir. Aynı şekilde Yaş="35", Cinsiyet="E", İl="İzmir" olan kayda ait gelir bilgisi ile Yaş="50", Cinsiyet="E", İl="İzmir" olan kayıtların gelir bilgisi birbirleriyle değiştirilir. Böylece gerçeği yansıtmasa da istenilen istatistiki sonucu verebilecektir.

7.4.3.3. *Gürültü Ekleme* : Bu yöntem ile seçilen bir değişkende belirlenen ölçüde bozulmalar sağlamak için ekleme ve çıkarmalar yapılır. Bu yöntem çoğunlukla sayısal değer içeren veri kümelerinde uygulanır. Bozulma her değerde eşit ölçüde uygulanır. Örneğin; bir tablodaki "Gelir" sütunundaki değerler 45.000, 15.000 ve 100.000 ise her bir değer; (-5.000) çıkartılarak 40.000, 10.000 ve 95.000 olarak yansıtılabilir.

7.4.4. Anonim Hale Getirmeyi Kuvvetlendirici İstatistik Yöntemler

7.4.4.1. *K-Anonimlik* : Bir veri kümesindeki belirli alanlarla, birden fazla kişinin tanımlanmasını sağlayarak, belli kombinasyonlarda tekil özellikler gösteren kişilere özgü bilgilerin açığa çıkmasını engellemek için geliştirilmiştir. Bir veri kümesindeki değişkenlerden bazılarının bir araya getirilerek oluşturulan kombinasyonlara ait birden fazla kayıt bulunması halinde, bu kombinasyona denk gelen kişilerin kimliklerinin saptanabilmesi olasılığı azalmaktadır.

7.4.4.2. *L-Çeşitlilik* : K-anonimliğin eksikleri üzerinden yürütülen çalışmalar ile oluşan L-çeşitlilik yöntemi aynı değişken kombinasyonlarına denk gelen hassas değişkenlerin oluşturduğu çeşitliliği dikkate almaktadır.

7.4.4.3. *T-Yakınlık* : L-çeşitlilik yöntemi kişisel verilerde çeşitlilik sağlıyor olmasına rağmen, söz konusu yöntem kişisel verilerin içeriğiyle ve hassasiyet derecesiyle ilgilenmediği için yeterli korumayı sağlayamadığı durumlar oluşmaktadır. Bu haliyle kişisel verilerin, değerlerin kendi içlerinde birbirlerine yakınlık derecelerinin hesaplanması ve veri kümesinin bu yakınlık derecelerine göre alt sınıflara ayrılarak anonim hale getirilmesi sürecine T-yakınlık yöntemi denmektedir.

7.5. Kişisel Veri İçeren Fiziksel ve Sahipsiz Dokümanlar

Masa üstlerinde, yazıcılarda ve ofislerin çeşitli yerlerinde bırakılmış/unutulmuş bulunan fiziksel dokümanların sahiplerinin bulunamaması halinde, dokümanı ilk fark eden çalışan, işbu politikanın 6.2 maddesinde yer alan fiziksel kayıtların imha edilmesi esaslarına göre söz konusu dokümanı imha etmelidir.

8. Kişisel Verilerin Saklanması ve İşlenmesi İçin Alınan Teknik ve İdari Önlemler

Şirket, Kişisel verilerin düzgün şekilde saklanabilmesi ve güvenliğini sağlamak adına, kişisel verilerin niteliğini ve durumunu gözeterek, yetkisiz değiştirilmeyi, kaybolmayı muhtemel hasarı, izinsiz işleme veya erişimi, insan eylemi veya doğal veya fiziksel ortamın etkilerine maruz kalmak suretiyle ortaya çıkacak riskleri ve benzeri diğer zararları önlemek için fiziksel, teknik ve idari önlemler alır. Bunlara ek olarak;

8.1. Sızma (Penetrasyon) testleri ile Şirket bilişim sistemlerine yönelik risk, tehdit, zafiyet ve varsa açıklıklar ortaya çıkarılarak gerekli önlemler alınmaktadır.

8.2. Bilgi güvenliği olay yönetimi ile gerçek zamanlı yapılan analizler sonucunda bilişim sistemlerinin sürekliliğini etkileyecek riskler ve tehditler sürekli olarak izlenmektedir.

8.3. Bilişim sistemlerine erişim ve kullanıcıların yetkilendirilmesi, erişim ve yetki matrisi ile kurumsal aktif dizin üzerinden güvenlik politikaları aracılığı ile yapılmaktadır.

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

8.5. 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 yazılıma ilişkin (güvenlik duvarları, atak önleme sistemleri, ağ erişim kontrolü, zararlı yazılımları engelleyen sistemler vb.) önlemler alınmaktadır.

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

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

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

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

Commented [AA2]: Arkas Bilgi Sistemleri Direktörlüğü (BSD) şemsiyesi dışında kalan iştiraklerin irtibat kişileri 8. madde bütününde tarif edilen önlemleri kendi güncel uygulamalarına göre gözden geçirmelidir.
Eğer burada listelenen önlemler içinde uygulanamayanlar var ise, bunlar ilgili iştirakin politika metninden çıkarılmalıdır.

8.10. Kişisel verilerin hukuka aykırı olarak başkaları tarafından elde edilmesi halinde bu durumu ilgili kişiye ve Kurul'a bildirmek için Kurum tarafından buna uygun bir yöntem oluşturulmuştur.

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

8.12. Kişisel verilerin işlendiği elektronik ortamlarda güçlü parolalar kullanılmaktadır.

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

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

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

8.16. Özel nitelikli kişisel verilerin güvenliğine yönelik ayrı politika belirlenmiştir.

8.17. Özel nitelikli kişisel veri işleme süreçlerinde yer alan çalışanlara yönelik özel nitelikli kişisel veri güvenliği konusunda eğitimler verilmiş, gizlilik sözleşmeleri yapılmış, verilere erişim yetkisine sahip kullanıcıların yetkileri tanımlanmıştır.

Commented [AA3]: Arkas Grubu dışında kalan iştiraklerde görev alan ve ÖNKV işleyen kişilere burada belirtilen eğitimlerin aldırılması gerekmektedir. "KVKK Eğitim Dokümanından" yararlanılabilir.

8.18. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği elektronik ortamlar kriptografik yöntemler kullanılarak muhafaza edilmekte, kriptografik anahtarlar güvenli ortamlarda tutulmakta, tüm işlem kayıtları loglanmakta, ortamların güvenlik güncellemeleri sürekli takip edilmekte, gerekli güvenlik testlerinin düzenli olarak yapılması/yaptırılması, test sonuçlarının kayıt altına alınması gerçekleştirilmektedir.

8.19. Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği fiziksel ortamlar için güvenlik önlemleri alınmakta, yetkisiz giriş çıkışlar engellenmektedir.

8.20. Özel nitelikli kişisel veriler e-posta yoluyla aktarılması gerekiyorsa şifreli olarak kurumsal e-posta adresiyle veya KEP hesabı kullanılarak aktarılmaktadır. Taşınabilir bellek, CD, DVD gibi ortamlar yoluyla aktarılması gerekiyorsa kriptografik yöntemlerle şifrelenmekte ve kriptografik anahtar farklı ortamda tutulmaktadır. Farklı fiziksel ortamlardaki sunucular arasında aktarma gerçekleştiriliyorsa, sunucular arasında VPN kurularak veya SFTP yöntemiyle veri aktarımı gerçekleştirilmektedir. Kağıt ortamı yoluyla aktarımı gerekiyorsa evrakın çalınması, kaybolması ya da yetkisiz kişiler tarafından görülmesi gibi risklere karşı gerekli önlemler alınmakta ve evrak "gizli" formatta gönderilmektedir.

8.21. Asgari olarak Şirket politikalarına ve Şirket'in faaliyet gösterdiği alanda uygulanan teamüllere uygun güvenlik önlemleri alınır.

8.22. Tüm çalışanlar, işledikleri bütün Kişisel verilerin güvenli şekilde tutulmasını temin etmekle yükümlüdürler. Kişisel veriler, kazaen veya başka bir şekilde de olsa herhangi yetkisiz bir üçüncü kişiyle sözlü, yazılı veya başka şekilde paylaşılamaz, ifşa edilemez.

8.23. Çalışanların, Kişisel Verileri yetkisiz olarak paylaşmaları ve bu Politika'da geçen gerekliliklere aykırı hareket etmeleri halinde bu durumun derhal Veri Sorumlusu İrtibat Kişisi'ne bildirilmesi gerekmektedir. Bu durum genellikle bir disiplin cezası gerektirebilir ve/veya duruma göre çalışanın İş Kanunu'nun 25. maddesi uyarınca iş akdinin haklı sebeple feshine neden olabilir.

8.24. Kişisel Veri içeren fiziksel kopyalar kilitli dolaplarda veya kilitli çekmecelerde tutulmalı; elektronik kopya ise [lütfen buraya "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikasının" linkini ekleyiniz.] yer alan tüm güvenlik kriterleri uygulanmalıdır.

8.25. Kişisel Veriler elektronik veya fiziksel kopya olsun personelin evinde, dizüstü bilgisayarlarda veya diğer kişisel taşınabilir cihazlarda ve işyeri dışındaki diğer sahalarda tutulamaz.

8.26. Normal şartlar altında, Kişisel verilerin personelin evinde, dizüstü bilgisayarlarda veya diğer kişisel taşınabilir cihazlarda veya diğer uzak yerlerde tutulmayacak olmasına rağmen, işyeri sahası dışında tutmanın gerekli veya uygun olduğuna şirket yönetimi tarafından onay verilirse, çalışanlar "Bilgi Sistemleri Genel Standartlar ve Güvenlik Politikasında" yer alan tüm güvenlik kriterlerine uymalıdır.

8.27. Taşınabilir elektronik cihazlarda veya silinebilir ortamlarda depolanan verilerden söz konusu ekipmanı yöneten çalışan sorumludur. Bu kişi, aynı zamanda aşağıdaki unsurları sağlamakla yükümlüdür:

8.27.1. İlgili cihazlarda ve ortamlarda yer alan verilerin zarara uğrama ihtimallerine karşılık bu verilerin yeterli güvenlik önlemlerinin alındığı ortamlarda saklanan yedeklerinin olması,

8.27.2. Özel nitelikli kişisel verilerin ve diğer hassas verilerin uygun şekilde şifrelenmiş olması,

8.27.3. Veri Sorumlusu İrtibat Kişisi veya Veri Yetkilisi'ne danışmadan özel nitelikli kişisel verilerin veya diğer hassas verilerin taşınabilir depolama cihazlarına kopyalanmamış olması ve bu bağlamda ilgili şifreleme ve koruma önlemlerinin alınmış olması ve,

8.27.4. Özel nitelikli kişisel verileri ve diğer hassas verileri içeren dizüstü bilgisayar, mobil cihazlar ve bilgisayar bazlı kayıt ortamlarının (USB cihazları, CD'ler gibi) ofiste gözetimsiz bırakılmaması.

8.27.5. Çalışanlar, güvenli Şirket programları üzerinde kayıtlı olan, kişisel veri içeren belgeleri gerekmedikçe kullandığı bilgisayara kopyalayamaz ve/veya indiremez, indirdiği ve/veya kopyaladığı takdirde ise işleme amacı bittiğinde, düzenlediği belge şirket tarafından kullanılacaksa şirket sunucularına ve/veya ilgili programlara kaydedildiğinden emin olduktan sonra söz konusu elektronik kopyayı derhal siler.

9. Uygulama

9.1. Yayımlama : Bu Politika çalışanlara Veri Sorumlusu tarafından sunulacaktır.

9.2. Yürürlük Tarihi : Bu Politika yayımlandığı anda yürürlüğe girer.

9.3. Değişiklikler : Bu Politika'da gerçekleştirilecek değişikliklerin öncesinde, Veri Sorumlusu İrtibat Kişisi veya Veri Yetkilisi, Veri Sorumlusu'ndan talepte bulunabilir. Politika değişiklikleri Veri Sorumlusu tarafından yapılır.

10. Politikanın Saklanması

Veri Sorumlusu, bu Politika'yı yayınlamak ve saklamakla yükümlüdür. Her departman yöneticisi bu Politika'nın uygulanmasından sorumludur. Bu Politika'nın uygulanmasıyla ilgili olan sorular Veri Sorumlusu İrtibat Kişisi ve Veri Yetkilisi'ne yönlendirilmelidir.

11. Politikanın İhlali ve İhlal İncelemesi

11.1.1. Bir çalışanın bu Politika'ya uyumu sağlayamaması halinde, departman yöneticisi tarafından aşağıdakileri belirleyebilmek adına inceleme yapılır. Gerekli görüldüğü takdirde, Politika'nın Şirket'e etkisi değerlendirilerek ihlalinden kaynaklanan riski azaltmak için uygun düzenleyici önlemler alınır. İhlalin ciddiyeti dikkate alınarak, çalışanın [lütfen buraya "Disiplin

Yönetmeliğinin" linkini ekleyiniz.] 'de yer alan bir disiplin yaptırımına (işten çıkarılma ihtimalini de içerir) tabi olup olmayacağı belirlenir.

Commented [AA4]: Arkas Grubu dışında kalan iştirakler eğer dilerlerse (ve varsa) kendi disiplin yönetmeliklerini buraya linkleyebilirler.

11.1.2. İhlali takip eden eylemlerin uygun olduğuna karar verilmesi halinde, departman yöneticisi Veri Sorumlusu İrtibat Kişisi, Üst Yönetim ve İnsan Kaynakları Direktörlüğü ile bağlantıya geçer ve gerekli eylemleri uygulamak için harekete geçer.

ÖZEL İTALYAN ANA VE İLKOKULU
KİŞİSEL VERİ SAKLAMA VE İMHA POLİTİKASI
6.11.2019 / Versiyon No: 1

EK-A / Saklama ve İmha Süreleri Tablosu

Commented [AA5]: Arkas Bilgi Sistemleri Direktörlüğü (BSD) şemsiyesi dışında kalan iştiraklerin irtibat kişileri EK-A'da yer alan süreç, saklama ve imha süresi bilgilerini envanterlerinde yer alan bilgilere ve VERBİS kayıtlarına göre gözden geçirmelidir.
Eğer gerekliyse işbu tablodaki verileri envanter ve VERBİS kayıtlarıyla aynı olacak şekilde revize etmelidirler.

SÜREÇ	SAKLAMA SÜRESİ	İMHA SÜRESİ
İş Sağlığı Güvenliği Süreçlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip e ilk periyodik imha süresinde
Sözleşmelerin Süreçlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İletişim Faaliyetlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
İnsan Kaynakları Süreçlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Çalışan Adaylarına İlişkin Süreçlerin Yürütülmesi	Başvuru sürecinin sona ermesinden itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Siber Güvenlik Olay Yönetimi	Kayıt altına alınmasını takiben 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Donanım ve Yazılıma Erişim Süreçlerinin Yürütülmesi	Kayıt altına alınmasını takiben 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Ziyaretçi ve Toplantı Katılımcıların Kaydı	Etkinliğin sona ermesini takiben 2 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Kamera Kayıtları	Kayıt altına alınmasını takiben 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Müşteri Verileri	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Tedarik Süreçlerinin Yürütülmesi	İş ilişkisinin sona ermesinden itibaren 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Muhasebe ve Finans Süreçlerinin Yürütülmesi	Kayıt altına alınmasını takiben 15 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Genel Kurul ve Yönetim Kurulu İşlemleri	Kayıt altına alınmasını takiben 10 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Resmi ve Hukuki İşlemlerin Yürütülmesi	Hukuki ilişkinin sona ermesinden itibaren 20 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Seyahat Süreçleri	Seyahatin sona ermesinden itibaren 1 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde
Posta, Kargo, Gönderi Kayıtları	Kayıt altına alınmasını takiben 5 yıl	Saklama süresinin bitimini takip eden ilk periyodik imha süresinde

EK-B / Saklama ve İmha Sürecinde Yer Alan Kişiler Tablosu

Commented [AA6]: Arkas Bilgi Sistemleri Direktörlüğü (BSD) şemsiyesi dışında kalan iştiraklerin irtibat kişileri EK-B'da yer alan unvan, birim ve görev bilgilerini güncel organizasyon yapıları ve uygulamalarına göre gözden geçirmelidir.
Eğer tabloyu revize etmelidirler.

Şirket'in tüm çalışanları Politika'nın uygulanması ve bu Politika'da yer alan teknik ve idari tedbirlerin alınması konusunda sorumlu kişilere aktif olarak destek vermekle yükümlüdür.

UNVAN	**BİRİM**	**GÖREV**
Genel Müdür	Yönetim	Çalışanların politikaya uygun hareket etmesinden sorumludur.
KVK Danışma Grubu	Risk Yönetimi, İnsan Kaynakları, Bilgi Sistemleri, Kurumsal Stratejiler	Politika'nın hazırlanması, geliştirilmesi, yürütülmesi, ilgili ortamlarda yayınlanması ve güncellenmesinden sorumludur.
Veri Sorumlusu İrtibat Kişisi	-	Veri sorumlusu nezdinde politikanın yürütülmesinden sorumludur.
Bilgi Sistemleri Direktörü	Bilgi Sistemleri Güvenliği	Politika'nın uygulanmasında ihtiyaç duyulan teknik çözümlerin sunulmasından ve gerekli yatırımların sağlanması için yönetimin bilgilendirilmesinden, elektronik kayıt ortamlarında gerçekleştirilen silme, yok etme, anonimleştirme işlemleri bakımından yürütme ve iç denetimlerden sorumludur.
İnsan Kaynakları Direktörü	İnsan Kaynakları, İdari İşler, Güvenlik	Görevlerine uygun olarak politikanın yürütülmesinden, Arşiv, Güvenlik gibi diğer birim sorumlularını ve çalışanları denetlemekle sorumludur.