ANEMON

KİŞİSEL VERİLERİN KORUNMASI KANUNU

TEKNİK TEDBİRLER RAPORU

İÇİNDEKİLER

YÖNETİCİ ÖZETİ

Kişisel Verilerin Korunması Kanunu Teknik Tedbirler Hukuki Uyumluluk Programı'nın temel amacı, ANEMON HOTELS **("ANEMON ", "Şirket" veya "Kurum")** 'nin, 7 Nisan 2016 tarihinde yayımlanarak yürürlüğe giren 6698 sy. Kişisel Verilerin Korunması Kanunu **("KVKK" veya "Kanun")** kapsamında teknik tedbirler hukuki uyumluluğunun birincil ve ikincil düzenlemeler dahil olmak üzere gerçekleştirilmesidir. Bu amaçla ANEMON bilgi sistemleri alt ve üst yapısı üzerinde Mevzuatta belirtilen usul ve esaslara uygun olarak mevcut durumun tespiti, yeterliliği ve uyumluluğu hakkında görüş oluşturulması ve sonuçların işbu KVKK Teknik Tedbirler Süreç ve Planlama Raporu **("Rapor")** 'na aktarılması hedeflenmiştir.

Rapor, ANEMON bilgi sistemleri, bileşenleri ve süreçleri dahilindeki özel ve genel nitelikli kişisel veriler başta olmak üzere son kullanıcı verisine temas eden tüm bilgi, belge ve varlıkları kapsamaktadır.

Asıl olarak 3 kısımdan oluşan raporun;

- **1. Kısım** kapsamı düz yazı ve paragraf biçiminde **tespit ve önerilerimizi** içermektedir,
- **2. Kısım** KVKK Projelerinin 3 boyutunu ortaya koyan **GRC** (Governance-Risk-Compliance) Süreç, Risk ve Uyum proje kartlarından oluşmaktadır. Bu kısımdaki değerlendirmeler ilk kısımdaki tespitlerin biraz daha detaylandırılmış ve görsel olarak kolay ulaşılır hale getirilmiş bir başvuru doküman setidir.
- **3. Kısım** olan "Teknik Tedbir Prosedürleri" başlığı altında ise Veri Koruma Politika ve Prosedür metinlerine ve işbu Rapor 'un ekleri olarak hazırlanan **harici prosedürlere** de yer verilmiştir.

Ayrıca KVKK ve ilgili mevzuat dahilinde teknik tedbirler için temin edilmesi gereken yeterlilikleri sağlama çalışmaları halihazırda devam etmekte olup ANEMON Bilgi Teknolojileri **("IT")** ve Teknik İşler Birimi ile yapılan ikili değerlendirme toplantıları ve bunun yanında diğer birimler ile yapılan koordine toplantılar kapsamında Kanun karşısındaki uyumluluğun sağlanmasına yönelik karşılıklı hedef tedbir seviyeleri belirlenmiştir.

Bu itibarla; işbu Rapor bu hedeflere ulaşabilmek amacıyla hazırlanan yol haritasını ortaya koymaktadır. İzleyen başlıklar, teknik tedbirler kapsamında rehber olabilecek hukuki kontrol ve önerileri içermektedir.

ANEMON HOTELS

TEKNİK TEDBİRLER RAPORU

Teknik ve İdari Tedbirlere İlişkin Genel Açıklamalar

Giriş

Teknolojinin hayatlarımızı kolaylaştırması gerçeğiyle birlikte günümüzde hemen her işletmede kişisel ya da ticari tüm veriler dijital ortamlarda tutulmaya başlanmıştır. Dolayısıyla dijital ortamlardaki veri güvenliğini sağlamak zorunlu bir haline gelerek bilişim sistemlerinin güvenliği kurumlarda en öncelikli konulardan biri olmuştur.

ANEMON 'un sunmakta olduğu hizmetlerde çok etkili bir şekilde teknolojiyi kullandığı ve kişisel verilerin dijital ortamlarda tutulduğu anlaşılmaktadır.

Kişisel Verileri Koruma Kurumu tarafından öngörülmüş birtakım teknik tedbirler kurumların veri güvenliği politikalarının yapısında bir çeşit çatı vazifesi görmektedir. Yapının temelleri sağlam olmadan çatının gerektirdiği hassasiyeti göstermek mümkün olmayacaktır.

İşbu rapor, bu kapsamda şirketin temas ettiği kişisel verilerin Kanun 'a ve mevzuatına uygun olarak korunmasını hedefleyen ve bunu yanında ANEMON HOTELS güvenilir bir Veri Sorumlusu konumuna getirmek amacıyla özellikle yeniden değerlendirilerek dikkatlerinize sunulmuş tespit ve öneri niteliğindeki değerlendirmeleri içermektedir. Ancak önemle belirtmek gerekir ki bu değerlendirmeler kalıcı olmayıp dinamik ve sürekli güncellenmek zorunda olan notlardır. İşbu çalışma Mart 2020 tarihi itibarı ile cari ve etkindir.

Amaç ve Dayanak

6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun **12. madde**sinin birinci fıkrasında;

"Veri sorumlusu;
a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,
b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,
c) Kişisel verilerin muhafazasını sağlamak

amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır." hükmü yer almaktadır. Bu kapsamda, kişisel verilerin işlenmesi sürecinde veri sorumlusu olarak ANEMON 'un alması gereken idari ve teknik tedbirler bulunmaktadır.

Kapsam

İşbu Teknik Tedbirler Raporu, 6698 Sayılı Kişisel Verilerin Korunması Kanunu'na Uyumluluk Projesini yürütmekte bulunduğumuz ANEMON 'un uyumluluğunun sağlanması adına Kişisel Verileri Koruma Kurumu'nun Ocak 2018'de yayınlamış olduğu ''Kişisel Veri Güvenliği Teknik ve İdari Tedbirler Rehberi'' baz alınarak hazırlanmıştır. Bu Rapor, ANEMON Bilgi Teknolojileri süreçlerinde kişisel veri barındıran sistemlerde uygulanması gereken idari ve teknik tedbirlere yer vermektedir.

Veri kayıt sistemlerinde kişisel veri işlenmesi sürecinde bu verilerin güvenliğine ilişkin çeşitli riskler ortaya çıkabilmektedir. Bu risklerin önüne geçilebilmesi için yeterli zaman, verimli kaynak kullanımı ve alanında uzman ekiplerden yardım sağlanarak uygun teknik ve idari tedbirlerin alınması gerekmektedir. Söz konusu önlemlerin bir kısmı maliyet gerektirmekte, bir kısmı ise maliyet gerektirmeden alınabilmektedir.

Raporumuz kişisel verilerin hukuka aykırı olarak işlenmesinin ve kişisel verilere hukuka aykırı olarak erişilmesinin önüne geçilerek kişisel verilerin güvenli bir biçimde muhafazasının sağlanması ve bireylerin temel hak ve özgürlüklerinin korunmasının temini için veri sorumlusu olarak ANEMON 'a yol göstermesi amacıyla hazırlanmış olup, bu kapsamda alınabilecek teknik ve idari tedbirleri ihtiva etmektedir. Söz konusu raporda öncelikle Kişisel Verileri Koruma Kurumu'nun belirttiği idari ve teknik tedbirlerin genel açıklaması yapılmış, sonrasında ise Şirket bünyesindeki bilgi teknolojileri süreçlerine dair mevcut durum analizi yapılarak tespit ve önerilerde bulunulmuştur.

Mevcut durum analizi, ANEMON bilgi teknolojileri biriminin beyanına göre şekillendirilmiştir. ANEMON IT bilgi teknolojileri süreçleri, söz konusu beyanlara dayanılarak sadece Kişisel Verileri Koruma Kurumu'nun öngördüğü süreçlere ilişkin olarak **değil**; aynı zamanda **ISO 27001** ve **5651** sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanunun gereklilikleri yönünden de irdelenmiştir.

Tanımlar

- **Veri Sorumlusu:** Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi olarak ANEMON A.Ş. 'dir.
- **Kişisel Verilerin İşlenmesi:** Kişisel verilerin manuel veya bir otomasyon sisteminin parçası olarak elde edilmesi, kaydedilmesi, depolanması, muhafazası, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi kişisel veri üzerinde gerçekleştirilen her türlü işlemdir.
- **Veri İşleyen:** ANEMON A.Ş. 'nın verdiği yetkiye dayanarak onun adına kişisel verileri işleyen, ANEMON organizasyonu dışındaki gerçek veya tüzel kişilerdir.
- **İlgili Kişi:** Kişisel verisi işlenen gerçek kişidir.
- **İmha:** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesidir
- **Kanun:** 24/3/2016 tarihli ve 6698 Sayılı Kişisel Verilerin Korunması Kanunu'dur.
- **Veri Kayıt Sistemi:** Tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işlenen kişisel verilerin bulunduğu her türlü ortamdır.

- **Kişisel Veri Saklama ve İmha Politikası:** Veri sorumlularının, kişisel verilerin işlendikleri amaç için gerekli olan azami süreyi belirleme işlemi

ile silme, yok etme ve anonim hale getirme işlemi için dayanak yaptıkları politikadır.

- **Kişisel Veri Güvenliği:** Kişisel veri ve kişisel veri işleme sistemlerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz kişilerin veriye ulaşmaları halinde tespit edilmelerine yönelik tedbirlerin tümüdür.
- **Bilgi Güvenliği Yönetim Sistemi (BGYS):** Kurum içerisinde var olan Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, yazılı hale getirilmiş, kurumun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütünüdür.
- **Kullanıcı:** ANEMON IT merkez ve bütün hizmet yerlerinde bulunan kişisel veri ve kişisel veri işleme tesislerine erişen tüm kişilerdir.
- **Siber Olaya Müdahale:** Bilgi sistemleri ve endüstriyel kontrol sistemleri veya bu sistemlerde tutulan veya işlenen verilerin gizlilik, bütünlük veya erişilebilirliğinde meydana gelme riski bulunan veya meydana getirilen siber olayın kaynağını, nedenlerini ve sonuçlarını tespit ederek siber olayın devam etmesini, tekrarını veya zarar vermesini önleyen çalışmalardır.
- **Sistem Odası:** Bilgisayar sistemleri, ağ ve depolama cihazları gibi ekipmanların bulunduğu ortamdır.
- **Ağ Erişim Kontrol (NAC):** Kullanıcıların ağa erişimini kontrol altına almak ve yetkilendirmek için kullanılan çözümdür.
- **Veri Sızıntısı Önleme (DLP):** Hassas verilerin kaybını engellemeyi hedefleyen bir teknolojidir. Veri kaynağında, dolaşımda yahut kullanımdayken bilginin konumlandırılması, sınıflandırılması ve izlenmesine odaklanılmasına sağladığı imkanla; bir kuruluşun hangi bilgilere sahip olduğunun saptanması meydana gelmesi muhtemel veri sızıntılarınının engellenmesini sağlamaktadır.
- **Hotspot:** Kamusal olan ve olmayan alanlarda kablosuz yerel ağlardan internete ortamına erişimi sağlayan bölgedir.
- **Güvenlik Duvarı:** Gelen ve giden ağ trafiğini izleyen ve belirli güvenlik kuralları kümesine göre hangi trafiklere izin verilip verilmeyeceğine karar veren bir ağ güvenlik aygıtıdır.
- **DMZ:** Bir kuruluşun güvenilir iç ağı ile internet gibi güvenilir olmayan dış ağı arasındaki ayrıştırılmış özel alandır.
- **Kurumsal Kaynak Planlama (ERP):** Kurumun sahip olduğu kaynakları planlamasına imkan sunarak verimli kullanabilmesini sağlayan bir sistemdir.
- **Web Servis:** HTTP protokolü üzerinden platform gözetmeksizin diğer sistemlere veya cihazlara hizmet veren yapıdır.
- **SSL:** Çevrimiçi iletişimde bir web sunucusu ve bir tarayıcı arasında şifrelenmiş bağlantılar oluşturmak için kullanılan standart bir güvenlik protokolüdür.
- **IP:** Verilerin internette bir bilgisayardan diğerine gönderildiği yöntem veya protokoldür. İnternetteki ve Intranetteki her bilgisayar, diğer tüm bilgisayarlardan benzersiz şekilde kendisini tanımlayan en az bir IP adresine sahiptir.
- **İstemci:** Bir hizmetin alıcı ucu yahut bir istemci / sunucu model sistem türünde faaliyet gösteren bir hizmet istemcisidir.
- **İnternet Servis Sağlayıcısı (İSS):** İnternet ile ilgili hizmetleri sunan firmaya veya kuruma denir.
- **MAC Adresi:** Bir ağ üzerinden Ethernet veya ağ bağdaştırıcısı için benzersiz bir tanımlayıcıdır. Farklı ağ arayüzlerini ayırt eder ve birçok ağ teknolojisi için, özellikle Ethernet dahil olmak üzere çoğu IEEE 802 ağında kullanılır.
- **Sunucu:** İstemci olarak bilinen başka bir program tarafından yapılan istekleri kabul eden ve yanıtlayan bir bilgisayar programı veya aygıtıdır.
- **Veri Tabanı:** Bir bilgisayar programının istenen veri parçalarını hızla seçebileceği şekilde düzenlenmiş bir bilgi topluluğudur.
- **Log:** Sistemlerdeki herhangi bir olayın veya hareketin kayıtlarını ifade eden terimdir.

Mevcut Risk ve Tehditlerin Belirlenmesi

Kişisel verilerin güvenliğinin sağlanabilmesi için öncelikle ANEMON tarafından işlenen tüm kişisel verilerin neler olduğu belirlenerek, bu kişisel verilerin korunmasına ilişkin ortaya çıkabilecek risklerin gerçekleşme olasılığı ve gerçekleşmesi durumunda yol açacağı kayıplar göz önünde bulundurularak uygun tedbirlerin alınması noktasında çeşitli tespitlerde bulunulmuştur.

Bu risklerin belirlenmesinden sonra, söz konusu risklerin azaltılması ya da ortadan kaldırılmasına yönelik tespitlerde bulunularak çeşitli çözüm alternatifleri; düşük maliyet, uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmiş, ANEMON nezdinde gerekli teknik ve idari tedbirlerin planlanarak uygulamaya konulması hususunda Şirket 'e çeşitli tavsiyelerde bulunulmuştur.

Çalışanların Eğitilmesi ve Farkındalık Çalışmaları

Kişisel verilerin güvenliğini zedeleyecek saldırılarda, çalışanların sınırlı bilgileri olsa dahi ilk müdahaleyi yapmaları kişisel veri güvenliğinin sağlanması hususunda çok büyük önem taşımaktadır.

Kişisel veri güvenliğini ihlal etmeye yönelik saldırıların yanı sıra, kullanıcıların tecrübesizlik, dikkatsizlik veya dalgınlık gibi zayıf yönlerinin kullanılması suretiyle kötücül yazılım içeren e-posta ekinin açılması veya e-postanın yanlış alıcıya gönderilerek kişisel verilerin üçüncü kişilerin yetkisiz erişimine açılması şeklinde, kişisel verilerin hukuka aykırı olarak açıklanması ya da paylaşılması gibi konular başlıca kişisel veri güvenliği ihlalleri olarak belirtilebilir.

Bu nedenle kişisel veri güvenliğinin sağlanabilmesi için öncelikli olarak ANEMON A.Ş. 'nın çalışanları, kişisel verilerin hukuka aykırı olarak açıklanmaması ve paylaşılmaması gibi konular hakkında kurum içi kapsamlı bilgi güvenliği eğitimleri, çalışanlara yönelik farkındalık çalışmalarının periyodik olarak planlanması ve yapılması **tavsiye edilir**.

Hukuk Büromuz olarak yürütmekte olduğumuz 6698 sayılı Kişisel Verilerin Korunması Kanunu'na Uyumluluk Projesi kapsamında ANEMON IT nezdinde çalışan herkesin kişisel veri güvenliğine ilişkin rol ve sorumluluklarının bilincinde olarak; çalışanların kişisel veri işlenen faaliyetleri yürütürken hassas davranmaları ve bu noktada rol ve sorumluluğun farkına varılmasının sağlanması amaçlanmış, çalışanlardan kaynaklı kişisel veri ihlallerinde çalışana rücu edilebilmesi için işe alınma süreçlerinde gizlilik anlaşmaları imzalamaları **tavsiye edilir**.

Kişisel Veri Güvenliği Prosedürlerinin Belirlenmesi

Kişisel veri güvenliğine ilişkin olarak uygulanabilir bir politika hazırlanması risklerin önceden belirlenebilmesini ve belirlenen risklere daha hedefli bir şekilde önlem alınmasını sağlayacaktır.

ANEMON 'un çalışma ve işleyişine uygun şekilde entegre edilecek kişisel veri güvenliğinin sağlanmasına yönelik belirlenecek doğru ve tutarlı politika ve prosedürler uzun uğraşlar sonucunda ortaya çıkartılan tespit ve analizlerin uygulanabilir olmasının en etken yöntemleridir.

Bu konudaki politika ve prosedürler şirketin dinamiklerine göre güncellenmeli, periyodik olarak kontroller gerçekleştirilmeli, yapılan bu kontroller belgelendirilmeli, geliştirilmesi gereken hususlar belirlenmelidir. Gerekli aksiyonlar yerine getirildikten sonra dahi **düzenli kontrollere** devam edilmelidir.

Personelin, belirlenen güvenlik politika ve prosedürlerine uymaması halinde devreye girecek disiplin süreci işletilerek; kişisel veri güvenliği ihlalleri yaşanması halinde personelin maruz kalacağı disiplin cezaları **düzenlenmeli ve tebliğ edilmelidir**.

Ayrıca belirtmek gerekir ki; kişisel veri güvenliğine ilişkin hazırlanan politika ve prosedürlerde önemli değişikliklerin meydana gelmesi durumunda; çalışanlara bildirimde bulunularak, onların kişisel veri güvenliğine ilişkin tehditler hakkındaki bilgilerinin güncel tutulması adına yeni eğitimler yapılması **sağlanmalıdır**.

Kişisel Veri İhtiva Eden Belge ve Ortamların Mümkün Oldukça Sadeleştirilmesi

Kanun'un 4. maddesinin 2. fıkrasının (b) ve (d) bentleri uyarınca kişisel veriler, gerektiğinde doğru ve güncel olmalı, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir.

Uzun süredir faaliyet gösteren veri sorumlusu ANEMON tüzel kişiliği özellikle personellerine ve müşterilerine ait kişisel veriler başta olmak üzere satış sonrası, e-ticaret ve takip/şikayet kanallarından fazla miktarda kişisel veri toplamaktadır. Bu kişisel verilerin bir kısmı zamanla güncelliğini yitirmiş, doğru olmayan ve herhangi bir amaca hizmet etmeyen kişisel veriler olmakla birlikte diğer bir kısmı ise özel nitelikli kişisel veriler içermektedir.

Bu durumun önüne geçebilmek için, Şirket 'in [1]söz konusu kişisel verilere hala ihtiyacı olup olmadığını değerlendirmesi ve [2]bu kişisel verilerin Kanun 'un ve rehberlerinin tanımladığı seviyede güvenliklerinin temin edildiği şekilde muhafaza edildiğinden emin olması gerekmektedir.

Son olarak yetkisiz erişimin engellenebilmesi için veri sorumlusu ANEMON 'a sıklıkla erişimi gerekmeyen ve arşiv amaçlı tutulan kişisel verilerin daha güvenli ortamlarda muhafaza edilmesi ve ihtiyaç duyulmayan kişisel verilerin kurum Kişisel Veri Saklama ve İmha Politikasına uygun olarak *(Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında)* Yönetmelik'e uygun ve güvenli bir şekilde imha edilmesi gerekmektedir.

Veri İşleyenler ile Kurulacak ya da Devam Eden İlişkiler Bakımından Kanun'un Uygulanması

ANEMON bilgi teknolojileri ihtiyaçlarını karşılamak için veri işleyenlerden çeşitli konularda hizmet alımı gerçekleştirmektedir. ANEMON 'un hizmet alımı yapılmadan önce söz konusu veri işleyenlerin (kişisel verilerin korunması konusunda) ANEMON tarafından sağlanan güvenlik seviyesine muadil bir güvenliği sağlandığından emin olması gerekmektedir.

Şirket bünyesinde Ürün Dışı Satın Alma Birimi mevcut olmakla bu konuda sağlıklı bir kanal yaratılmıştır.

Zira Kanun'un 12.maddesinin 2. fıkrası gereği veri sorumlusu olarak ANEMON 'dan almış olduğu yetkiyle veri işleyenler de kişisel verilerin güvenliğinin sağlanması konusunda veri sorumlusu ANEMON ile birlikte **müştereken sorumludur**.

Bu husus göz önünde bulundurularak; ANEMON IT dış kaynaklı hizmet alımı gerçekleştirdiği firmalarda **KVKK uyumluluğu aramalıdır.**

Veri işleyen ile imzalanan sözleşmenin **yazılı olması**, veri işleyenin sadece kişisel verilerin korunması mevzuatı ile uyumlu bir şekilde, veri sorumlusu ANEMON 'un talimatları doğrultusunda, sözleşmede belirtilen veri işleme amaçlarına uygun hareket edeceğine ilişkin **hüküm/ler içermesi** ve bu sözleşmelerin ANEMON 'un Kişisel Verilerin Korunması Politikası 'na **uygun olması** önemli önerilerimiz arasında yer almaktadır.

İşlenen kişisel verilere ilişkin olarak **veri işleyenlerin süresiz sır saklama yükümlülüğü altında bulunduğunun** sözleşmede yer alması tavsiye edilir. Ayrıca; söz konusu sözleşmede herhangi bir kişisel veri ihlali olması durumunda, **veri işleyenin bu durumu derhal veri sorumlusu ANEMON A.Ş. 'ye bildirmekle yükümlü olduğunun belirtilmesi** de, veri sorumlusu ANEMON 'un bu ihlali derhal Kişisel Verileri Koruma Kurumu'na ve ilgili kişiye bildirme yükümlülüğünü yerine getirmesi açısından kritik olacaktır. (bkz. https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi).

Ayrıca; taraflar arasındaki sözleşmenin niteliği buna elverdiği ölçüde, ANEMON tarafından veri işleyene aktarılan kişisel verilerin sözleşmede tür ve kategori olarak ayrı bir maddede belirtilmiş olması, veri işleyenin veri güvenliğini sağlama yükümlüğünü yerine getirmesi açısından faydalı olacaktır.

Siber Güvenliğin Sağlanması

Tehditlerin her an nitelik ve boyut değiştirerek etki alanlarını genişlettiği günümüz dünyasında tek bir siber güvenlik ürünü kullanımı ile kişisel veri güvenliğinin sağlanabilmesi mümkün değildir. İnternet gibi ortamlardan gelen saldırılara karşı ilk savunma hattı olarakrehberde de önemle vurgulandığı üzere; [1]güvenlik duvarı ve [2]ağ geçidi kişisel veri içeren ortamlara karşı internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasını sağlayan öncelikli tedbirler olarak listenin başında yer almaktadır.

Şirketin yapısı ve ihtiyaçlarına uygun olarak yapılandırılmış bir güvenlik duvarı (ANEMON 'da mevcuttur[+]), kullanılmakta olan ağa gerçekleşecek ihlalleri henüz zarar gerçekleşmeden durdurabilir. Bunun yanında İnternet Ağ Geçidi alt yapısı (ANEMON 'da mevcuttur[+]) ise çalışanların, kişisel veri güvenliği bakımından tehdit teşkil eden internet sitelerine veya online servislere erişimini önleyerek teknik tedbirler rehberinde de yer verilen ve beklenen önemli güvenlik unsurlarındandır.

Güvenliğin sağlanabilmesi açısından yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları bulunmakta olup, kullanılmayan yazılım ve servislerin cihazlardan kaldırılması potansiyel güvenlik açıklarının azalmasını sağlamaya yardımcı olacaktır. Bununla beraber her yazılımın ve donanım bir takım kurulum ve yapılandırma işlemlerine tabi tutulmalıdır. Ancak burada özellikle sıklıkla, kullanımı gerekmeyen yazılımların güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikle tercih edilebilecek bir yöntemdir. (ANEMON 'da mevcuttur ancak düzenli aralıklarla kontrol ve takip edilmelidir).

Zararlı yazılımlara karşı güvenliğin sağlanabilmesi için, sistem ağını düzenli olarak kontrol eden ve tehlikeleri saptayan antivirüs, antispam gibi çözümlerin kullanılması gerekmektedir (ANEMON 'da mevcuttur^{+}). Fakat söz konusu uygulamaların fabrika ayarları ile kurulumu yeterli olmayıp kurum özeline göre çeşitli ayarlamalar yapılarak aktifleştirilmesi gerekmektedir.

Kişisel verinin gerektiğinde doğru ve güncel olmasının sağlanmasının yanı sıra bu sistemlerin düzgün bir şekilde çalışması ve alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol edilmesi, olası güvenlik açıklarının kapatılması için yama yönetimi ve yazılım güncellemelerinin temini (ANEMON 'da mevcuttur^{+}) de hassasiyetle takip edilmelidir.

Ayrıca, kişisel veri içeren sistemlere erişimin de sınırlandırılması gerekmektedir. Bu kapsamda çalışanlara, kullanıcı adı ve şifre kullanılmak suretiyle yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmalıdır. Söz konusu şifre ve parolalar oluşturulurken, kolaylıkla tahmin edilemeyecek kişisel bilgilerle ilişkili olmayan büyük küçük harf, rakam ve sembollerden oluşacak parolaların tercih edilmesi sağlanmalıdır (ANEMON 'da mevcuttur^{+}).

Ayrıca idari tedbirlerin teknik tedbirlerle iç içe geçtiğinin güzel bir örneği olarak da İlişikleri kesilen çalışanlar için vakit kaybedilmeden hesapların silinmesi ve erişimlerin kaldırılması gerekmektedir. Güçlü parola ve şifre kullanımının yanı sıra, kaba kuvvet algoritması (BFA) kullanımı gibi yaygın saldırılardan korunmak için şifre girişi deneme sayısının sınırlandırılması, düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması, yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması gerekmektedir. (ANEMON 'da mevcuttur ancak düzenli aralıklarla kontrol ve takip edilmelidir). Yine, farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, söz konusu bağlantıların SSL VPN veya sFTP ya da varsa şirkete ait daha özel bir kanal üzerinden gerçekleştirilmesi güvenliğin korunması bakımından Kanun a daha uygun olacaktır.

Kişisel Veri Güvenliğinin Takibi

Şirket bilgi teknoloji sistemleri içeriden ve dışarıdan gelen saldırılar başta olmak üzere çeşitli siber saldırılara ve zararlı yazılımlara maruz kalabilir. Ancak söz konusu ihlaller birtakım göstergelere rağmen anlaşılamayabileceği gibi müdahale için de geç kalınabilir. Bu durumun önüne geçebilmek için;

a) Bilişim ağlarında ne türde yazılım ve servislerin barındırıldığının (yazılım envanteri) kontrol edilmesi,
b) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının (sızma ve zafiyet testleri) belirlenmesi,
c) Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi),
d) Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması,
e) Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması'' gerekmektedir.

Söz konusu raporlar, sistem tarafından oluşturulabilecek otomatik raporlar olabileceği gibi bu raporları ve muhtemel alarmları koordine ederek ve ilişkilendirerek (corelation) sistem yöneticisine ileten yetenekli yazılımlar da olabilir. (-ANEMON 'da mevcut değil)

Ayrıca, güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi, bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zaafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması gerekmektedir. (ANEMON 'da mevcuttur+).

Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

Kişisel veri ihtiva eden kayıtlar ANEMON 'un yerleşkelerinde yer alan cihazlarda ya da kağıt ortamı gibi fiziksel ortamlarda saklanıyor ise, bu cihazların ve kağıtların kaybolması veya çalınması gibi tehditlere karşı fiziksel güvenlik önlemlerinin alınması suretiyle korunması gerekmektedir. Aynı şekilde, kişisel verilerin yer aldığı fiziksel ortamların dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunması ve bu ortamlara giriş / çıkışların kontrol altına alınması gerekmektedir. (ANEMON 'da mevcuttur+)

Aynı seviyedeki önlemlerin ANEMON IT yerleşkesi dışında yer alan ve ANEMON 'a ait kişisel veri içeren kağıt ortamları, elektronik ortam ve cihazlar için de alınması gerekmektedir. (ANEMON 'da mevcuttur+)

Elektronik ortamda tutulan kişisel veriler ise, kişisel veri güvenliği ihlalini önlemek için ağ bileşenleri arasında erişim sınırlandırılabilir veya bileşenlerin ayrılması sağlanabilir. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil, sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilecektir.

Çalışan personele ait şahsi cihazların şirket bilgi sistemleri ağına bağlanmasının getireceği birtakım riskler hesaba katılarak yeterli güvenlik tedbirlerinin alınması gerekmektedir. Kişisel veri güvenliğine ilişkin ihlaller daha çok bu verileri içeren dizüstü bilgisayar, cep telefonu, flash disk vb. cihazların çalınmasıyla ortaya çıksa da elektronik posta başta olmak üzere fiziki posta yolu ile aktarılacak kişisel verilerin de kontrollü bir şekilde ve KVKK Teknik Tedbirler Rehberinde yer alan öneriler dikkate alınarak gönderilmesi gerekmektedir. (ANEMON 'da mevcuttur+)

Ayrıca söz konusu kişisel verilerin yeterli korumaya tabi tutulabilmesi için bu verileri içeren kağıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek koruma tedbirlerinin alındığı başka bir yere alınması, kullanılmadığı durumlarda kilit altında bırakılması, giriş çıkış kayıtlarının tutulması gibi fiziksel güvenliğin arttırılmasına ilişkin tedbirler de alınmalıdır. (ANEMON 'da mevcuttur ancak düzenli aralıklarla kontrol ve takip edilmelidir).

Kişisel veriye hukuka aykırı olarak erişilmesini önlemek adına kağıt ortamındaki verilerin kilitli şekilde muhafaza altına alınmalı ve sadece yetkili kişilerin erişimine açılmalıdır Ayrıca kişisel veri içeren cihazların çalınması başta olmak üzere kaybolması ihtimali gibi durumlara karşı şifreleme yöntemleri kullanılmalı ve bu kapsam erişim yetkilendirme departmanları tarafında yetki matrisi kapsamında erişim konrol yetkilendirmesi kullanılmalıdır. (ANEMON 'da mevcuttur ancak düzenli aralıklarla kontrol ve takip edilmelidir).

Bununla beraber rehbere bakıldığında şifrelemenin ''farklı formlarda kullanılan ve bu formlara göre farklı şartlar sağlayan bir güvenlik sağlama aracı'' olduğu ifade edilmektedir. Cihazda yer alan bir belge şifreleneceği gibi, tam disk şifreleme yöntemi kullanılarak cihazın tümü de şifrelenebilir. Ancak sektörde yer alan bazı yazılımların verilerde değişiklik yapılmasına engel olduğu kişisel verinin yetkisiz kişiler tarafından okunmasını durduramamaktadır. Bu nedenle söz konusu rehberde; ''hangi şifreleme yöntemleri kullanılırsa kullanılsın kişisel verilerin tam olarak korunduğundan emin olunmalı ve bu amaçla uluslararası kabul gören şifreleme programlarının kullanılmasına özen gösterilmesi'' ifade edilmiştir. Ayrıca ''tercih edilen şifreleme yönteminin asimetrik şifreleme yöntemi olması halinde, anahtar yönetimi süreçlerine önem gösterilmelidir'' denilmektedir. Tavsiyemiz ANEMON bünyesinde özellikle mobil cihazlarda "**Full Disk Encryption**" yani tam disk şifreleme teknolojisinin kullanılmasıdır. (ANEMON 'da mevcuttur ancak geliştirilmesi gerekmektedir).

Kişisel Verilerin Bulutta Depolanması

Teknolojinin sağladığı kolaylıklarla beraber kayıt sistemlerimizin yapısı değişerek dijital dünyaya taşınmaktadır. Bu kapsamda sürece bakıldığında işletmelerin öncelikle kendi yapılarında kurdukları veri merkezleri bulut bilişimden faydalanılarak dış kaynak kullanılmasına doğru evrilmektedir. Her işletmenin mevcut ihtiyaçlarına göre biçimlendirilebilmesinin yanı sıra; ekonomik olması sebepleriyle her geçen gün daha çok tercih edilen bulut bilişim ile beraber, İşletmeler kendi asıl ihtiyaç alanlarına özel modern çözümlere yönelebilmektedir.

Bulut bilişim; bilgisayar sistemleri başta olmak üzere veri işleme, depolama ve diğer faaliyetlerin yürütülmesi için gereken kaynakların üçüncü bir gerçek ya da tüzel kişiden temin edilmesidir. Bu kapsamda bakıldığında bu hizmeti sağlayan ve bu hizmetten faydalanan tarafların birtakım hakları bulunmaktadır.

Bulut bilişim alanının hukuki problemleri özellikle üç ana başlık altında toplanmaktadır;

1. İlk olarak kullanıcının bulut bilişime yüklemiş olduğu verilerin telif hakları başta olmak üzere çeşitli ticari sırlar barındırması sebebiyle fikri mülkiyet haklarına haiz olmasıdır.
2. İkinci olarak bulut bilişim yapısında barındırdığı devasa makine gücünün sürekli enerji tüketmesi ve bu enerji kullanımı ile beraber çevresel sorunlara sebebiyet vermesi nedeniyle çevre hukukunu da ilgilendirmektedir.
3. Son olarak bu sistemlere yüklenen verilerin kişisel veri barındırması nedeniyle kişisel verilerin korunması hukukunu da ilgilendirdiği görülecektir.

Bir yapının bulut olabilmesi için aşağıdaki hususları taşıması gerekmektedir:

- Bekletmesiz bir şekilde kullanıcıya hizmet verme, kullanıcıların ihtiyaç duydukları her an her yerden bu hizmetten yararlanabilmesi,
- Geniş ağ erişimi
- Kaynak havuzu tüm kullanıcılarını istedikleri zaman herhangi bir fiziksel ya da sanal kaynakla sınırlı olmaksızın hizmet modelini değiştirebilmesi
- Hızlı esneklik kullanıcı ihtiyaç duyduğunda kendisine otomatik olarak fazladan kullanım alanının sağlanması
- Ölçülebilir bir hizmet veya kullanıldığı kadar ödeme imkanı

Bulut bilişim; kullanıcı taleplerine göre arttırılabilen ya da azaltılabilen oranda bir ağ üzerinden bilişim kaynaklarının sağlanması hizmetidir. Kullanıcılar bu teknolojiden faydalanmak istediklerinde genel olarak bilişim teknolojilerini kendileri satın almak yerine başka bir üçüncü kişiden kiralama yoluna başvurmaktadır.

Kişisel verilerin bulutta depolanması, hukuka aykırı işlemenin ve erişimin önlenmesi ile hukuka uygun muhafaza yükümlülüğü olan ANEMON ’un kendi bilgi teknolojileri sistemi ağından ayrılmasına ve kişisel verilerin bulut depolama hizmeti sağlayıcıları tarafından işlenmesine neden olabileceğinden, bu durum birtakım riskleri beraberinde getirecektir.

KVKK, bulut depolama hizmeti sağlayıcısı tarafından alınan güvenlik önlemlerinin de yeterli ve uygun olup olmadığının değerlendirilmesini ANEMON tarafına yüklemektedir.

Dolayısıyla söz konusu kişisel verilerin bulut ortamında korunabilmesi için, bu ortama aktarılan kişisel verilerin neler olduğunun detaylıca bilinmesi, yedeklenmesi, senkronizasyonun sağlanması ve bu kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama yöntemleri ile erişim sağlanması tavsiye edilmektedir.

Bulut ortamına aktarılacak kişisel verilerin depolanması ve kullanımı sırasında, kriptografik yöntemlerle kilitlenmesi, bulut ortamlarına kilitlenerek atılması, kişisel veriler için mümkün olan yerlerde, ‘’özellikle hizmet alınan her bir bulut çözümü için ayrı ayrı şifreleme anahtarları kullanılması’’ gerektiği Kişisel Verileri Koruma Kurumu tarafından yayınlanan ‘’Kişisel Veri Koruma İdari ve Teknik Tedbirler Rehberi’’ nde belirtilmiştir.

Ayrıca söz konusu rehberde, bulut bilişim hizmet ilişkisinin sona ermesi halinde; kişisel verileri erişilebilir hale getirmeye yarayabilecek anahtarlarının tüm kopyalarının da yok edilmesi gerekmektedir.

Bilgi Teknolojileri Sistemleri Tedariği, Geliştirme ve Bakımı

ANEMON IT tarafından yeni bilgi teknolojileri sistemlerinin tedariği, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar saptanırken, uluslararası veri güvenliği standartlarında yer bulan güvenlik kıstaslar göz önünde bulundurulmalıdır.

Şirketlerin yapısı göz önünde bulundurulduğunda kurum içi kaynak kullanılarak geliştirilen uygulamaların sınırlı sayıda olduğu bu manada, şirketlerin daha çok dışardan tedarik yöntemine başvurarak ihtiyaçlarını gidermeye çalıştıkları görülmektedir. Ancak dışardan tedarik edilen uygulama ve sistemlerin kurulumu başta olmak üzere yaşanan teknik sıkıntılarda hizmet alımı yapılan şirket tarafından, sistemlere erişim sağlanmakta dolayısıyla kişisel veriye yetkisiz erişim ihtimali ortaya çıkmaktadır. Uzaktan destek hizmetleri yürütülürken bu ihtimal göz önünde bulundurularak, canlı ortam ve test ortamlarının oluşturulması ve firmaların bu kapsamda test ortamına alınması gerekmektedir.

Kişisel Verilerin Yedeklenmesi

Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi gerekmektedir.

Ayrıca rehberde, yedeklenen kişisel verilerin sadece sistem yöneticisi tarafından erişilebilir olması, veri seti yedeklerinin ise muhakkak surette ağ dışında tutulması gerektiği belirtilmiştir. ''Aksi halde, veri seti yedekleri üzerinde kötü amaçlı yazılım kullanımı veya verilerin silinmesi ve yok olması durumlarıyla karşı karşıya kalınabilecektir. Bu nedenle tüm yedeklerin fiziksel güvenliğinin de sağlandığından emin olunmalıdır'' denilmektedir.

ANEMON yapısında yedekleme (backup) teknolojisi olarak Network NAS yazılımı kullanmakta ve yedekleme planı olarak her gün Full Backup alınmaktadır. Ayrıca haftalık, aylık ve yıllık yedekler de alınmaktadır. Yıllık Backup 'ların arşivi Hem lokalde hem de TR'de bir bulut sağlayıcıda farklı bir lokasyonda muhafaza edilmektedir.

İlave olarak, kötücül yazılımlar da halihazırda sistemlere zarar vererek kişisel verilerin erişilebilirliğini etkilemektedir. Örneğin elektronik cihazlarda kişisel verileri içeren dosyaları kilitleyerek fidye ödemeye zorlayan çeşitli zararlı yazılımlar bulunmaktadır. Bu tür zararlı yazılımlara karşı kişisel veri güvenliğinin tesis edilebilmesi için veri yedekleme stratejilerinin geliştirilmesi gerekmektedir. ANEMON özelinde her gün full backup alınması bu risk bakımından oldukça güvenli bir ortam sağlamaktadır. Ayrıca güvenlik kameralarının internete açık olmaması ANEMON Bilgi İşlem departmanı tarafından uygulanan son derece yerinde bir uygulamadır ziara bu tür (ransomware-fidye) ataklarının kullandığı yöntem zayıf işlemcili kolaylıkla exploit (etkisiz hale getirerek aynı kanaldan sızma) 'ya müsait güvenlik kameralarıdır.

KVKK TEKNİK TEDBİRLER ÇÖZÜM MATRİSİ (REFERANS YAZILIMLAR)

TEKNİK TEDBİR	YÜKÜMLÜLÜKLERİ KARŞILAYAN ÜRÜN REFERANSLARI (ÖRNEKTİR)
Yetki Matrisi	IBM Identity & Access Manager, Solarwinds ARM, Veritas Data Insight
Yetki Kontrol	IBM Identity & Access Manager, Cyberark EPM, Solarwinds ARM, Veritas Data Insight
Erişim Logları	IBM Qradar, Arcsight, Logsign, TrendMicro Deep Security (File Integrity Monitoring, Log inspection), Manage Engine ve Solarwinds Yazılımları, Veritas Data Insight
Kullanıcı Hesap Yönetimi	Cyberark Yetkili Hesap ve Şifre Yönetimi Çözümleri (Vault, PSM, EPM), Centrify, Thycotic, ObserveIT
Ağ Güvenliği	Cisco Ağ Güvenliği Çözümleri(ISE,Firepower,Sourcefire,Umbrella,Stealthwatch), NAC Çözümleri FortiNAC, Forescout NAC, APT Çözümleri Trend Micro DDI, Fireeye NX
Uygulama Güvenliği	IBM Appscan, Fortify, NOD32 Endpoint and Device Control, Web application firewall çözümleri (Imperva, Forti Web), Cyberark EPM
Şifreleme	NOD32 Drive, File, Removable Media Encryption, Trendmicro Encryption, Symantec PGP Encryption, Sophos SafeGuard
Sızma Testi	Pentest Hizmeti, IBM Qradar Vulnerability Manager, QRadar Risk Manager, Nessus Security Center, Picus Security, Normshield
Saldırı Tespit ve Önleme Sistemleri	Cisco Sourcefire IPS, Trend Micro Tipping Point IPS, TrendMicro Deep Security (Host IPS), NOD32 IPS, Fireeye APT, TrendMicro APT, Forti DDOS, Arbor DDOS
Log Kayıtları	IBM Qradar, Arcsight / Logsign, Forti SIEM, Surelog / TrendMicro Deep Security (Log inspection)
Veri Maskeleme	Microfocus Voltage, Control Point ve SDM, M-Files, Secupi, IBM Guardium, Imperva
Veri Kaybı Önleme Yazılımları	Symantec DLP, Forcepoint DLP, NOD32 DLP / Veri Sınıflandırma: Symantec ICT, Boldon James, Titus, Microsoft AIP / FileOrbis dlp entegre doküman yönetimi
Yedekleme	Network NAS, Veritas Backup Exec
Güvenlik Duvarları	Palo Alto, Fortigate, Checkpoint, Cisco Firepower, Sophos
Güncel Anti-Virüs Sistemleri	Symantec Endpoint, Trendmicro Officescan, NOD32 EPO, Cisco AMP, Kaspersky
Silme, Yok Etme veya Anonim Hale Getirme	Microfocus Control Point ve SDM (Veri Yönetimi), M-Files(Doküman ve İçerik Yönetimi), FileOrbis(Yapılandırılmamış Veriler ve Doküman Yönetimi), Ground Labs(Hassas Veri Keşfi) Dataguise(Veritabanı Sınıflandırma ve Güvenlik), Secupi(Anonimleştirme, Silme), OmniSuite(KVKK İzin Yönetimi)
Mail Güvenliği	Cisco Email Security Appliance (ESA), Symantec Brightmail, Forcepoint Email Gw, TrendMicro hosted Email Security, TrendMicro DDEI, Fireeye EX
Mobil Cihaz Güvenliği	MDM Çözümleri Airwatch, MobileIron, Meraki MDM, IBM Maas360
Yetkilendirme/ 2 Factor Authentication	Forti Authenticator, Gemalto, Watchguard Authpoint, Symantec, Cisco DUO

ANEMON KVKK Teknik Tedbirler Tablosu

Yetki Matrisi – File Server için mevcut. ERP ve CRM için de oluşturulacak.	
Sanallaştırma - VmWare 6.7 - 3 fiziksel host, 40 sanal sunucu, 1 fiziksel yedekleme sunucusu	
Erişim Logları - Sunucularda Windows Event Log'ları tutuluyor, Netsis te SQL üzerinden log kayıtlarına firmadan destek alınarak ulaşılabiliyor.	
Kullanıcı Hesap Yönetimi – Kullanıcı bazında periyodik kontrollerle yapılıyor.	
Ağ Güvenliği – Firewall destekli ip bazlı erişim kontrolü mevcut. Ayrıca SAN – NAS çözümleri mevcut	
Uygulama Güvenliği – Kullanıcı bazında yetki güvenlik konfigürasyonu mevcut.	
Şifreleme – Bitlocker. (Gezen mobil notebooklara uygulanabilirlik şu anda mevcut değil. SOPHOS vb. çözümler için görüşülecek) $	
Sızma Testi – İç ve Dış Sızma Testi 1 yıllık periyotlarla yapılıyor. $	
Saldırı Tespit ve Önleme Sistemleri – Firewall + VPN ve diğer bazı yerel çözümler.	

Log Kayıtları – Log tutan sunucular olduğu halde bu makinaların ürettiği logları ve alarmları ilişkilendiren ve yöneten **SIEM** türevi yazılımları yok.	
Veri Maskeleme – Opera programı üzerinden kimlik bilgisi maskelenmekte. Ek olarak talep halinde maskeleme Ad Soyad ilk iki harf gerisi maskeli , kimlik no ilk iki ve son iki hane açık geri kalanı maskeli olarak yapılabilmekte , **Şu anda aktive edilmiş halde değil.**	
Veri Kaybı Önleme Yazılımları – Mevcut Değil	
Yedekleme - Network NAS (Full Back-up -her gün)	
Güvenlik Duvarı – ENDPOINT Firewall	
Güncel Anti-Virüs Sistemleri – NOD32	
Silme, Yok Etme veya Anonim Hale Getirme – Politika ve prosedür olarak mevcut. İmha ve Arşivleme için Profesyonel bir firmayla çalışılmıyor.	
Guest Network (Hotspot) 5651 s.k. – CryptoLog app.	

Veri Güvenliği (KVKK m.12) bakımından Tespitler

İşbu rapor; 6698 sayılı Kişisel Verilerin Korunması Kanununa dayanarak kurulan Kişisel Verileri Kurumu'nun; Ocak 2018'de yayınladığı ''Kişisel Veri Güvenliği Teknik ve İdari Tedbirler Rehberi'' baz alınarak hazırlanmıştır. Rehbere bakıldığında görülmektedir ki; kişisel veri güvenliği, veri güvenliğinin çatısı konumundadır. Veri güvenliğine ilişkin uluslararası standartlarda kabul edilmiş bilgi güvenliği kriterleri uygulanmadan kişisel veri güvenliği sağlanamayacaktır. Bu raporda; veri sorumlusu statüsündeki ANEMON (Türkiye) ISO 27001 süreçlerinin gereklilikleri yönünden de sorgulanarak mevcut durum analizi yapılmış ve yöneticilere sunulmak üzere çeşitli önerilerde bulunulmuştur.

Mevcut Durum Kapsamında Tespit ve Öneriler

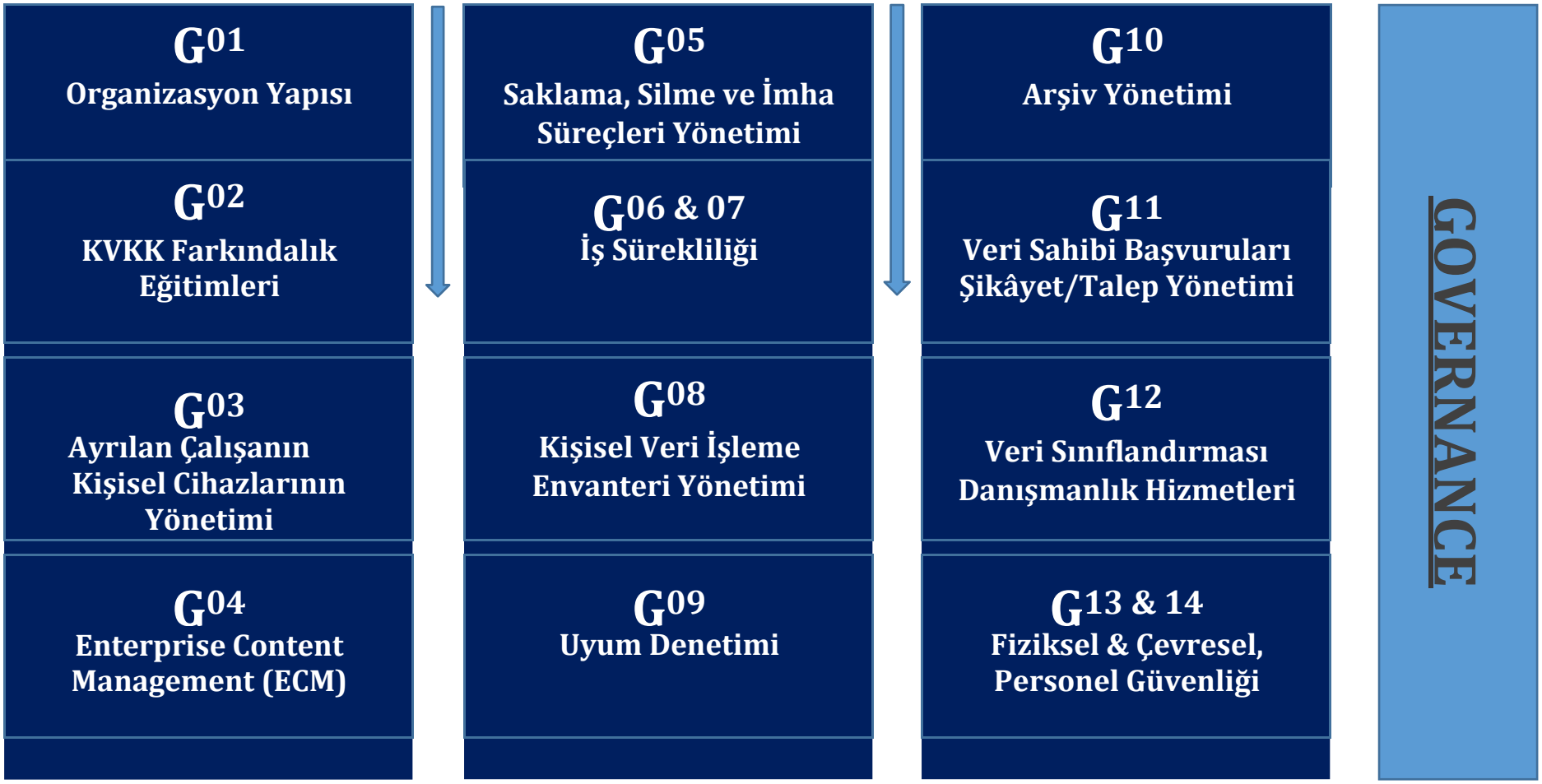
- ANEMON merkez yerleşkesine, servis sağlayıcı tarafından iki ayrı yedekli **fiber devre** tesis edilmiştir. İş sürekliliği kapsamında mevcut hatların, yedekleri ile birlikte tesis edilmiş ve yedeklilik testlerinin belirli periyotlarla yapıldığı bilgisi alınmıştır. İlgili data hatlarının ve bir kısım sistem envanterlerinin sonlandırıldığı ve konumlandırıldığı **kurum yerleşkesinde sistem odası bulunmakta olup sistem odası kart okuyucu sistemler ile sağlanmaktadır. Sistem odasının güvenliği için kamera kayıt sistemi bulunmaktadır**.
- VLAN 'lar, ağ yöneticilerinin, yeni kabloları çalıştırmak zorunda kalmadan veya mevcut ağ altyapısında büyük değişiklikler yapmadan, sistemlerin işlevsel ve güvenlik gereksinimlerini karşılayacak şekilde tek bir anahtarlı ağın bölümlendirilmesini kolaylaştırır. Anahtarlar üzerindeki portlar (ara yüzler) bir veya daha fazla VLAN 'a atanabilir, bu yapılandırma sistemlerin hangi departmanlar ile ilişkili olduklarına bağlı olarak mantıksal gruplara bölünmesini sağlar ve ayrı gruplardaki sistemlerin nasıl iletişim kurabileceğine dair kuralları belirler. ANEMON alt yapısında kullanıcı ve sunucu networkleri ayrı olup, tüm networkler firewall 'a ayrı bağlantılar olarak olarak tahsis edilmiştir. Bu şekilde tüm vLan 'ler firewall üzerinden haberleşebildiği için -iyi bir uygulama olarak, tüm network trafiği F/W 'dan geçerek iletişim sağlanıyor denebilir.

- Kurum yerleşkesinde an itibarı ile (Ekim 2022) Güvenlik Duvarı ürünü olarak **ENDPOINT UTM (Yeni Nesil) Güvenlik Duvarı** kurulu ve çalışır vaziyette olup lisans düzeyi olarak UTM (Birleşik Tehdit Yönetimi) içerecek şekilde lisanslanmıştır. Bu lisans türü bir anti-malware, içerik filtresi, güvenlik duvarı, izinsiz giriş tespiti rollerini tek bir pakete ekleyerek gerçekleştirmektedir. Ayrıca alt yapıda iki firewall olup birbirlerine yedekli çalışmaktadır,

- Tüm bu yetenekler mevcut fabrika ayarları ile değil KVKK m.12 'ye uygun güvenlik kriterleri ile ve yine şirkete uygun ayarlarla yapılandırılmalıdır. Bu konuda ilgili yetenekler özelinde dinamik ve periyodik eklentilerin kontrolü, uygulanması ve takip edilmesi tavsiye edilir.

- Yoğun trafiğin ve yüklü verinin dolaştığı ANEMON networkünde yüklerin otomatik dengelenmesini sağlayan bir load balance ürünü mevcut olmamakla birlikte High Availability (HA) özellikli uygulamalar bu güvenlik ihtiyacını desteklemektedir.

SÜREÇ ANALİZİ PROJE KARTLARI



Organizasyonel Yapılanma

Organizasyonel Aksiyon; KVKK'ya ilişkin gerekliliklerin takip edilmesi ve gerekli organizasyon aksiyonlarının zamanında alınması için en uygun organizasyon yapısına karar verilmelidir. Bu bir şirket içi komite ya da bu konuyla ilgili oluşturulmuş bir çalışma grubu olabilir. Karar verilen yapının şirket bünyesinde hayata geçirilmesi ile KVKK uyumluluğu önemli ölçüde sağlanmış olacaktır. Nitekim **ANEMON** İnsan Kaynakları Birimi liderliğinde yapılandırılan ve yürütülen KVKK Projesi sonucunda oluşturulan KVKK Komitesi yukarıda bahsi geçen unsurun sağlanması yolunda atılmış önemli bir adımdır.

Mevcut Durum: ANEMON bünyesinde ciddi ve düzenli çalışan bir KVKK çalışma grubu oluşturulmuştur.

EYLEM PLANI:

Şirket yapısı için en uygun organizasyon yapısı belirlenmelidir.

Belirlenen organizasyon yapısının hayata geçirilebilmesi için gerekli kaynaklar ayrılmalı ve mail grubu, periyodik toplantılar gibi planlamalar yapılmalıdır.

G02 R C KVKK Farkındalık Eğitimleri

KVKK hakkında çalışanların belirli bir farkındalık seviyesine ulaştırmak ve bu farkındalığı koruyabilmek adına yılda en az 1 defa olmak koşuluyla online eğitim platformları üzerinden veya fiili *(yüz yüze)* olarak KVKK farkındalık eğitimleri gerçekleştirilmelidir.

<u>Mevcut Durum</u>: ANEMON TR bünyesinde belirli aralıklarla KVKK ve Güncel durum hakkında eğitimler verilmektedir.

EYLEM PLANI:

KVKK farkındalık eğitimleri periyodik olarak sağlanabilir.

- *Eğitim için katılımcı listesinin hazırlanması.*
- *Eğitim sonunda uygulanacak ölçme değerlendirme sonuçlarının takibi.*

G03 R C Işe Başlayan-Ayrılan Çalışan Süreçlerinin Kontrolü

KVKK kapsamında, verilerin güvenliğini sağlayabilmek adına çalışanlara tahsis edilen tüm cihazların istihdamın sonlandırılması durumunda içerik kontrolleri sağlanmalıdır.

Mevcut durumda; **ANEMON** bünyesinde Ağ Cihazları Güvenlik Prosedürü bulunmakta ve ilgili prosedürde kullanıcı politikası yer almaktadır. Ayrıca gerekli zimmet formları da mevcut olmakla beraber mobil cihazlara ait yükümlülükler belirlenmiştir.

EYLEM PLANI:

Bu süreçle ilgili olarak Şirket bünyesinde haliz hazırda var olan prosedürlere muhtemel varyasyonları da kapsayacak şekilde bir güncelleme yapılacak olup işe girişte ve sonrasında tebliğ edilen kurallara ince ayar çekilecektir.

G04	R	C	Enterprise Content Management (ECM)

KVKK uyarınca kişisel veriler ancak işlendikleri süreç kapsamında geçerli olan amaç ve süre ile sınırlı olarak saklanmalıdır. Bu sebeple işleme amacı ortadan kalkmış veya belirlenen süreleri dolmuş kişisel verilerin kanun kapsamında silinmesi, imha edilmesi veya anonim hale getirilmesi en önemli ve ciddi yükümlülüklerdendir.

Proje kapsamında analiz edilen süreçlerde Kurum içi veri varlığının son adımı olan silme ve imha adımı kişisel verilerin işlenme amaç ve süreçleriyle bağdaştırılmamış olup, *mevcut durumda* ANEMON bünyesinde etkin bir silme/imha politikası oluşturulmuştur. Bunun yanında yapılandırıl**ma**mış veri olarak adlandırılılan verilerin tasnifi ve takibi için için ECM adı verilen ürün grubundan bir uygulama seçilerek bu alana hakimiyet sağlanacak şekilde konfigüre edilmelidir.

İçerik Yönetim Sistemleri (ECM) kişisel verileri işlenme amaçları ve kategorileri nezdinde tasnif ederek, sınıflarına göre alınacak silme/imha ya da anonimleştirme aksiyonlarının veri yaşam döngüsünün ilk aşamasında belirlemeye yardımcı olmaktadır. Mevcuttaki uygulamaların bu şekilde konfigüre edilmeleri verinin ömrünün (retention) belirlenmesi ve takibi açısından pratik yardımları olacaktır. Mevcut durumda belirli amaçlar için kullanılan EBA yazılımı sonraki güncellemelri ile bu amaca hizmet edecek modülleri kendisine eklemiştir. ANEMON 'daki versiyon

EYLEM PLANI:

Anemon bünyesinde kurulu olan EBA yazılımı bu ürün grubunda yer alan bir yazılımdır. Ancak hali hazırdaki version ve modüller bu ihtiyacı karşılayacak kapsamda değildir.
Bu ürün ya da başka bir yazılımla yapılandırılmamış veri alanı kontrol altına alınmalı ve gelişmiş bir teknik tedbir olarak bu yükümlülük karşılanmalıdır..

Saklama, Silme ve İmha Süreçleri Yönetimi

Kişisel veriler, Kanun ve ilgili diğer Kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde re'sen veya ilgili kişinin talebi üzerine silinmek, yok edilmek veya anonim hale getirilmek zorundadır. Bu nedenle hukuki tabanda mevzuata ilişkin ceza şartları tanımlanmış olup teknolojik anlamda da yaklaşımın güncel ve amaca hizmet edecek yöntemler üzerinden tercih edilmesi gerekmektedir.

Mevcut durumda ANEMON Kişisel Veri İşleme İç Envanterinde saklama süreleri veri tipleriyle eşleştirilerek mevzuatlardaki atıflara göre belirlenmiş ve belirli aralıklarla güncellenmektedir. Bunun yanında imha işlemleri için profesyonel bir firma ile anlaşılmış ve aksiyonlar tutanak ile kayıt altına alınarak ilerlenmektedir.

EYLEM PLANI:

Tespit edilen sürelerin dolması üzerine, verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin gerekli işlemlerin, veri saklama ve imha politikası ve oluşturulan kişisel veri işleme envanteri çerçevesinde yapılması çok önemlidir. ***Yapılmaması halinde TCK anlamında cezai sorumluluk doğması yolu açılacaktır.***

İş Sürekliliği – 1

- **İş Etki Analizi**

  İş etki analizi kritik IT sistemlerini ve risk bileşenlerini tanımlama ve önceliklendirme *(data dictionary)* süreçlerini kapsar.

- **Risk değerlendirme**

  Risk değerlendirme süreci organizasyonun kullanımdaki binaları, ekipmanları, teknolojisi, insan kaynağı ve 3.partileri ile ilgili muhtemel risklerin azaltılması ve/veya dengelenmesi için kontrollerin tanımlanmasına yardımcı olur ve bu kalan artık risklerin seviyesinin iş sürekliliği ve/veya felaket kurtarma planlaması yoluyla ele alınması süreçlerini kapsar.

- **Eğitim ve Güncelleme**

  İş sürekliliği konuları ile ilgili çalışanları eğitmeyi ve hazırlanan plan/prosedürlerin test edilme süreçlerini kapsar. Stratejiler ve planlar iş gereksinimlerinin değişme ihtimaline karşı güncel olması için düzenli olarak gözden geçirilme ve ihtiyaç halinde güncellenmelidir.

EYLEM PLANI:

İş operasyonları ve uygulamalar için periyodik iş etki analizi yapılmalı, potansiyel riskler belirlenmeli, sonuçları gözden geçirilmeli ve onaylanmalıdır. Mevcut durumda **ANEMON** *bünyesinde bu süreç uygulanmaktadır.*

İş sürekliliği standardı oluşturulmalı ve risk değerlendirme sürecini de içermelidir. Bu konuda rol ve sorumluluklar belirlenmeli, kritik sistemler ve iş birimleri için riskler belirlenip yıllık testler yapılmalıdır.

Strateji ve kurtarma planları yıllık olarak veya test öncesi güncellemelere ek olarak önemli değişiklik arz eden süreçler sonrasında güncellenmeli ve gözden geçirilmelidir. **ANEMON** *bünyesinde söz konusu süreç de periyodik yapılan testler sonrasında tespit edilen eksiklikler göz önünde bulundurulup güncellenmektedir.*

G07 R C İş Sürekliliği – 2

- **Kurtarma Stratejileri ve Uygulamaları**

  Kişisel verilerin depolandığı alanlar, veri merkezleri, bilgisayarlar ve uygulamalar için kurtarma stratejileri geliştirilmelidir. Kurtarma stratejisi uygulamaları ve sistemleri kurtarma hedeflerini iş birimleri nezdinde kurtarma hedefleri içerisinde kurtarmaya olanak sağlamalıdır.

- **Kurtarma Plan ve Prosedürleri**

  Kurtarma planları ve prosedürleri, veri merkezi, sistem, ağ ve/veya uygulamalar için detaylı rehber hazırlama sürecini kapsar.

- **Eskalasyon ve Kriz Yönetimi**

  İş kesintisine neden olabilecek herhangi bir olağanüstü olay yaşanması durumunda olayın etkin yönetilmesi için eskalasyon ve kriz yönetimi oluşturma süreçlerini kapsar.

Mevcut durumda ANEMON bünyesinde anılan 3 adım da gereği gibi yerine getirilmektedir. Yıllık periyodik testlerin sürdürülmesi ve ihtiyaç duyulabilecek yatırımların devamlılığı durumunda iş sürekliliği teknik/güvenlik tedbiri yerine getirilmiş sayılabilecektir.

EYLEM PLANI:

Ortak kurtarma referans mimarileri kurulmuştur. Kurtarma stratejileri, sistem, uygulama, iş sahası veya süreç kurtarma için gerekli her bir elementi yansıtmalıdır.

Hazırlanan iş sürekliliği planları periyodik olarak gözden geçirilmelidir. Kurtarma planları içerisinde olağanüstü hal durumunda nelerin yapılması gerektiği detaylı olarak belirtilmelidir.

Olay uyarısı ve alarm için otomatik bir araç kullanılabilir (Ayrıca bkz. R03 SIEM Proje Kartı) İş süreklilik planını uygulamak için bu yazılıma gerekli konfigürasyon yapılmalıdır.

Kişisel Veri İşleme Envanteri Yönetimi

KVKK Uyumluluk Projesi ve yol haritası çalışması kapsamında tüm departmanların katılımı ve katkılarıyla oluşturulmuş kişisel veri işleme envanterinin Şirket süreçleri değiştikçe güncellenmesi gerekmektedir. Bu envanter KVKK kapsamındaki denetim, veri sahibi başvurularının yanıtlandırılması ve veri koruması projesinin sürekliliğinin sağlanması amaçlarıyla kullanılmaya devam edilmelidir.

Aynı zamanda **ANEMON** özelinde Veri Sorumluları Sicil Bilgi Sistemi **("VERBİS")** kapsamında hazırlanan kişisel veri işleme iç envanteri VERBİS sistem girişlerinde esas alınmıştır. VERBİS sistemi iç envantere göre daha genel kriterler içeriyor olsa da kişisel veri işleme faaliyetlerinde herhangi bir değişiklik olması durumunda ilgili süreç VERBİS'e de doğru ve güncel olarak kaydedilmelidir.

EYLEM PLANI:

- *VERBİS ve kişisel veri işleme envanterinin güncellenmesinden sorumlu olacak kişilerin ve sorumluluklarının belirlenmesi,*
- *Denetim, veri sahibi başvurusu ve diğer kişisel veri işleme faaliyetleri kapsamında kişisel veri işleme envanterinin kullanım süreçlerinin belirlenmesi,*
- *Kişisel veri işleme envanteri kapsamında alınması gereken raporların ve kapsamlarının belirlenmesi.*

Uyum Denetimi

KVKK uyumluluğuna ilişkin kapsamlı denetimlerin veri sorumlusu tarafından yapılması ve/veya yaptırılması Kanun'da açıkça ifade edilmiştir. Bu doğrultuda, KVKK uyumluluğuna ilişkin denetim gerekliliklerinin belirlenerek, ilgili denetimin uygun periyodik aralıklarla, *örneğin yıllık,* olarak gerçekleştirilen denetim planı içerine dahil edilmesi KVKK'ya ilişkin ihlallere yol açabilecek durumların tespitini kolaylaştırmakla birlikte ihlal riskini de azaltacaktır. Aynı zamanda bu aksiyon, Kişisel Verileri Koruma Kurulu tarafından gerçekleştirilmesi beklenen dış denetimler öncesi Mevzuat uyumsuzlukların giderilmesi için önemli bir çalışma niteliğindedir.

EYLEM PLANI:

İlgili denetimin iç kaynaklarla gerçekleştirilmesi durumunda; kapsamının belirlenmesi, ihtiyaç duyulan adam/gün analizinin yapılması, yıllık denetim planı içerisine eklenmesi,

İlgili denetimin dış kaynaklı (outsource) bir firma tarafından gerçekleştirilmesi durumunda; bu firmaya karar verilmesi, denetim kapsamının belirlenmesi, ihtiyaç duyulan adam/gün analizinin yapılması, yıllık denetim planı içerisine eklenmesi gerekmektedir.

Arşiv Yönetimi

Veri Saklama ve İmha Politikası'nın olmaması, düzenli imha süreci gerçekleştirilmemesi, arşive iş birimi bazlı giriş yapılmaması ve dolayısıyla arşivdeki dokümanlara bütün Kurum çalışanlarının erişebilmesi, Kurum'un KVKK kapsamındaki risklerini arttırabilecek hususlardır. İmha politikasının oluşturulması, dijital arşive geçiş sürecinin başlatılması ve hukuka uygun imha süreçlerinin yürütülmesi sağlanmalıdır. Kişisel verilerin güvenliğinin sağlanması için arşive erişimlerin yetkilendirilmesi gerekmektedir.

İşbu raporun ekinde **ANEMON** adına Kişisel Veri Saklama ve İmha Politikası oluşturulmuş olup anılan ihlal riskleri bertaraf edilebilecektir.

Şirket datalarının yedeklemesi kartuşlara günlük, haftalık, aylık ve yıllık olarak alınmakta. Yıllık backuplar ise Hadımköy uzak lokasyonundaki ofiste güvenli bir kasada saklanmaktadır. Yedekler ise 6 ayda bir periyodik bakım planına göre teste tabi tutularak bütünlükleri ve doğrulukları kontrol edilmektedir.

EYLEM PLANI:

Arşivde gerçekleştirilecek iş birimi bazlı yetkilendirmeler ile kişisel veri ihtiva eden dokümanlara yetkisiz erişim engellenmelidir.

Kişisel Veri Saklama ve İmha Politikası güncel tutulmalıdır.

G11 R C Veri Sahibinin Başvurusu – Şikayet / Talep Yönetimi

KVKK kapsamında, şirkete bir çalışan aracılığıyla veya şirket bünyesinde kurulan KVKK Komitesi aracılığıyla gelen talep ve başvurulara kanun içerisinde belirlenen 30 günlük yasal süre içerisinde dönüş yapılabilmesi ve sürecin takip edilebilmesi adına etkin bir korelasyon sağlanmalıdır. Örneğin ortak bir mail havuzunun oluşturulması bu sürecin kontrol altına alınmasını ve hızlandırılması sağlayacak ve aynı zamanda doğabilecek riskleri minimize edecektir.

Halihazırda ANEMON bağlı diğer tüm lokasyonları da kapsayacak şekilde başvuru yönetim alt yapısı kurulmuştur.

EYLEM PLANI:

Şirketin tüm iletişim noktalarına erişimi sağlanacak şekilde veri sahiplerinin şikâyet ve taleplerini takip edebileceği bir çalışma grubu (komite) oluşturulması ve bu konuda şirketler genelinde farkındalığın yaratılması ve güncellenmesi önemli bir aksiyon olarak tesis edilmelidir.

G12 R C Veri İmha Sürecinde Danışmanlık Hizmetinin Alınması

Kişiisel Verilerin Korunması mevzuatında bir çok idari yaptırım (para cezası) mevcuttur. Ancak Kanun bazı durumlarda tedbir ve yaptırım seviyesini artırmış ve cezai yaptırıma (hapis) giden yolu açmıştır.

Kanuna göre "işleme amacını kaybeden kişisel verilerin ya silinmesi ya imha edilmesi ya da anonimleştirilmesi" gerekir. Yönetmeliğe ve rehberlerine göre düzenlenen bu kurallara uyulmaması durumunda TCK 135, vd. Hükümleri devreye girebilecektir.

EYLEM PLANI:

Mevcut durumda **ANEMON** bünyesinde saklama-imha ya da arşivleme faaliyetleri için profesyonel bir firmayla çalışma durumu olmadığı anlaşılmış olup ilerleyen dönemde önemli bir gündem olarak konuşulması tavsiye edilir.

G13	R	C	Fiziksel ve Çevresel Güvenlik

Departmanların iş gereksinimleri nedeniyle açık ofis ortamında sıkça kullandıkları matbu evrakları kilitli/şifreli dolaplar içerisinde muhafaza etmeleri, ilgili dokümanlara yetkisiz erişimi engellemiş olmanın yanında KVKK kapsamında teknik tedbir rehberinde tanımlanan önemli bir tedbiri gerçekleştirmektedir.

Mevcut durumda ANEMON bünyesinde fiziksel güvenlik oldukça yüksek seviyededir. Kameralar iş sağlığı ve güvenliği kurallarına uygun olarak yerleştirilmiş olup bu kayıtlar 1 ay tutulmakta ve sonrasında otomatik üzerine yazmaktadır (overwrite). Kameralar internete bağlı olmadığı önemli bir güvenlik aksiyonu olarak vurgulanmıştır.

Ek bilgi: *Fiziksel çevre ile alakalı tehditlere karşı destekleyici altyapıyı, binaları ve sistemleri koruma süreçlerini, bilgi depolama medyalarının (Laptop, USB ve sair), bilgi içeriğini ele vermeyecek şekilde yönetme, kontrol etme, taşıma ya da yok etme süreçlerini kapsar. Ekipmanlar çevresel tehditleri ve yetkisiz erişim fırsatlarını azaltmak amacıyla korunur.*

EYLEM PLANI:

- *İhtiyaç belirlenerek kilitli/şifreli dolaplar tedarik edilmelidir.*
- *Dolapların kilitlerini/şifrelerini muhafaza edecek sorumlular belirlemelidir.*
- *Dolap içerisinde barındırılan matbu evraklara erişimi takip edebilmek adına bu sorumlular görevlendirilmelidir.*

G14 R C Personel Kaynaklı Risk Güvenliği

Çalışan, sözleşmeli personeller ve üçüncü parti kullanıcılar için güncel yasalar, regülasyonlar, iş etiği ve ihtiyaçları, bilgi sınıflarına erişim ve risk algısına uygun olarak bütün adaylara arka plan kontrolleri uygulama süreçlerini kapsar.

Personel güvenliği ile ilgili gizlilik sözleşmesi, doküman ve politikaların personelin erişebileceği bir alanda tutulması, ilgili hukuki uyum ihtiyaçlarını içermesi ve her bir çalışanın en az yıllık olarak bu politikaları okuyup anladığını beyan etme süreçlerini ve iş birimlerinin bir araya gelerek şirket içerisinde personel tarafından oluşabilecek tehditlerin tartışılarak ihtiyaç halinde aksiyonların planlama süreçlerini kapsar. **Bu ve benzeri hassas belgelerin tutulduğu yazılım/uygulama ortamlarının güvenliğinin temini BT biriminin yükümlülüğüdür.**

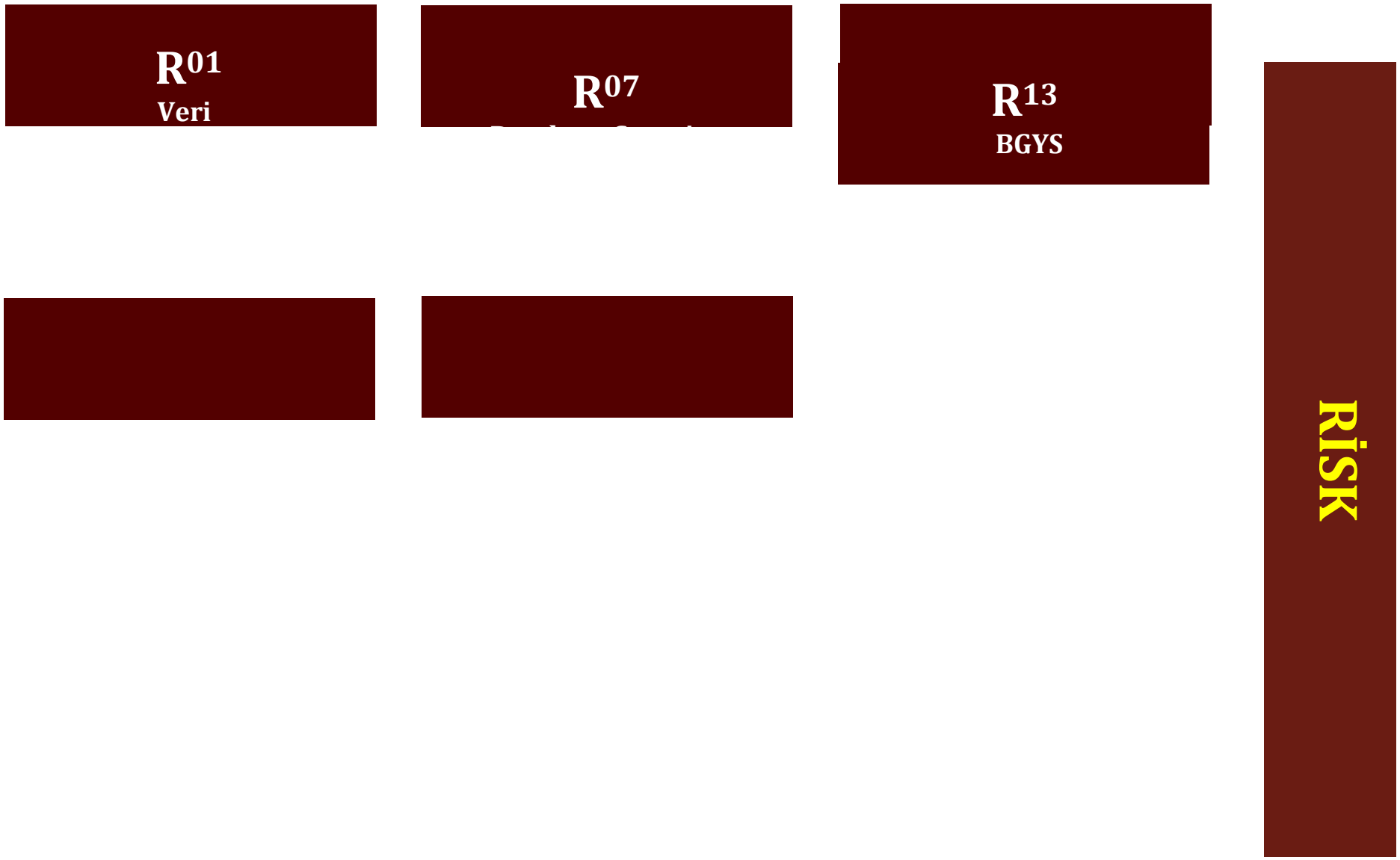
EYLEM PLANI:

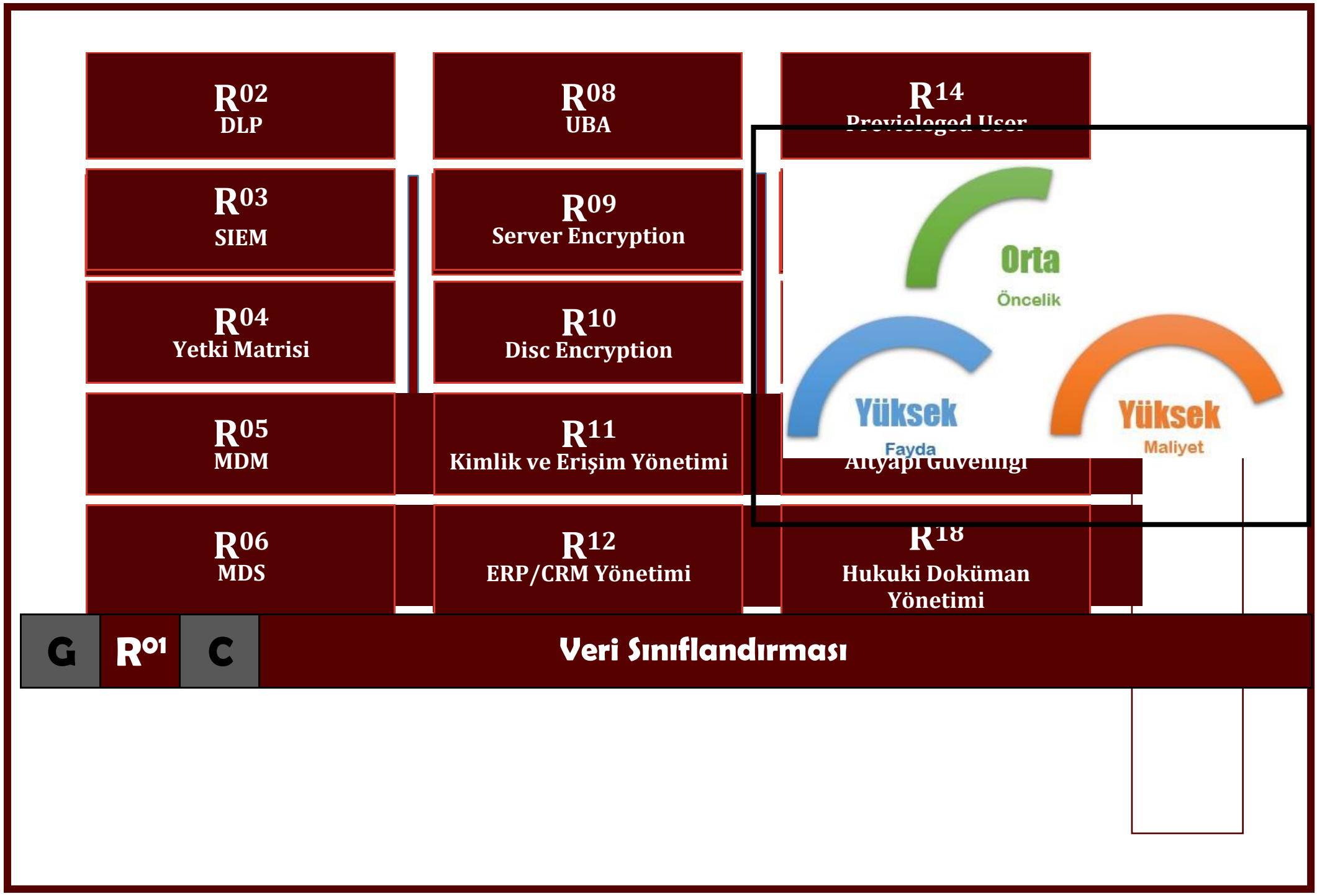
Bazı zorunlu personel güvenlik bilgi yönetim sistemleri ve ilave entegrasyon ve alarmlar yer almalıdır.

Güvenlik politikasını bütün personelin okuduğuna dair belgeleme mevcut olmalıdır. Bu süreç yıllık olarak alınan hukuki uyum eğitimi sonunda elektronik ortamda politikalara link vererek "okudum, anladım, onaylıyorum" ifadesi ile yönetilebilir.

İç tehdit azaltma için iletişim ve raporlama mekanizmaları mevcut olmalıdır. İç tehditleri tespit etmek için izleme prosedürleri bulunmalıdır ve bunlar geriye dönük araştırmaya veya anonim raporlamaya dayanmalıdır.

TEKNİK TEDBİRLER ANALİZİ PROJE KARTLARI




R02
DLP
R08
UBA
R14
Provisioned User
R03
SIEM
R09
Server Encryption
R04
Yetki Matrisi
R10
Disc Encryption
R05
MDM
R11
Kimlik ve Erişim Yönetimi
Altyapı Güvenliği
R06
MDS
R12
ERP/CRM Yönetimi
R18
Hukuki Doküman Yönetimi
Orta
Öncelik
Yüksek
Fayda
Yüksek
Maliyet
G
R01
C
Veri Sınıflandırması

sınıflandırılması gereklidir. Sınıflandırılan verilerin kullanıcılar tarafından rahatlıkla algılanabilmesi amacıyla yapılacak etiketleme çalışması için de veri sınıflandırmanın düzgün bir şekilde yapılması oldukça önemlidir. Sınıflandırılan veriler risk dereceleri ile eş değer güvenlik önlemleriyle korunabilir. Veri sınıflandırma, kurumsal risk yönetiminin önemli bir parçası olup özellikle Kanun ve hukuki uyum süreci için olmazsa olmaz bir gereksinimdir.

EYLEM PLANI:

Kuruma ait kişişel veri içeren tüm varlıklar sınıflandırılmalıdır. Veri sınıflandırma çalışması şirket IT ve Teknik İşler birimi tarafından teknoloji desteği verilerek konfigüre edilecek uygulama ile sağlanmalıdır.

Bu uygulamanın sağlanması akabinde ilgili iş birimleri iç kaynak ya da dış kaynak kullanımı ile mevcut veri işleme faaliyetlerinin etiketlenmesi ve kontrolünün sağlanması çalışmalarını yürüteceklerdir.

İlgili iş birimlerinin veri sınıflandırması kapsamında gerekli farkındalık eğitimini almış ve uygulama yönetimini ve gerekli girdiyi sağlayabilecek yeterlilikte olmaları beklenmektedir.

G	R02	C	Veri Kaybı Önleme – Data Loss Prevention (DLP)

KVKK m. 12 çerçevesinde veri sorumlusu;

- *Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,*
- *Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,*
- *Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.*

Veri güvenliği ile ilişkilendirilmiş idari para cezaları Kanun çerçevesinde 1.000.000 (bir milyon) Türk lirasına kadar tanımlanmıştır. Bu rakam üst sınır olmakla birlikte enflasyon oranında her yıl yeniden değerlenerek artışa göre uyarlanmaktadır.

Veri Sızıntısı Önleme *(DLP)* çözümleri, kurum için gizli ve kritik olan verinin, kurum dışına sızmasını önlemek amacıyla geliştirilmiştir. Verinin saklandığı ortamlarda *(dosya sunucusu, veri tabanı, CRM vb.)*, iletildiği ortamlarda *(E-mail, FTP, sosyal medya vb.)* ve kullanıldığı ortamlarda *(kullanıcı bilgisayarları, USB bellekler, akıllı telefonlar vb.)* saptanması, izlenmesi ve korunması için yardımcı olurlar. **ANEMON alt yapısında DLP mevcut değildir. Yeni nesil bir bundle olan ENDPOINT ortalama ancak doğru kurulduğunda yetenekli ve etkili bir çözümdür.**

EYLEM PLANI:

Veri Sızıntısı önleme çalışması Şirket IT ve Teknik İşler birimi tarafından teknoloji desteği verilerek ayrıca kurulacak olan bir uygulama ile sağlanacaktır.

Bu uygulamanın hayata geçirilmesi akabinde ilgili iş birimleri iç kaynak ya da dış kaynak kullanımı ile mevcut veri yönetişimi sürecinin işletilmesi ve kontrolünün sağlanması çalışmalarını yürüteceklerdir. İlgili iş birimlerinin veri sızıntısı önleme kapsamında gerekli farkındalık eğitimini almış ve uygulama yönetimini ve gerekli girdiyi sağlayabilecek yeterlilikte olmaları beklenmektedir.

R03 C Güvenlik Olay İzleme Yönetimi (SIEM)

Kurum bilgi sistemlerine yönelik olarak kötü niyetli kişilerce gerçekleştirilen saldırıların sayısı ve çeşidi her geçen gün artmaktadır. Kurumlar bu atakları çoğunlukla dışarıdan beklemekteyken atakların daha yıkıcı ve engellenemez olanları içeriden kaynaklanmaktadır. Bahsedilen teknik tedbir *(SIEM)* verinin tüm yönlerdeki tüm muhtemel hareketini takip ederek ve yorumlayarak çok kapsamlı bir şekilde kontrol altına alır.

- *Hangi bilgi sisteminden hangi logların alınacağı belirlenmelidir.*
- *Bu loglar bir sistem dahilinde bir araya getirilerek korele edilmelidir.*
- *Müdahale süreçleri, use case'ler ve playbook'lar oluşturulmalı ve karşılaşılan olaylara göre iyileştirilmelidir.*
- *Olay müdahalenin etkinliğini artırmak için tehdit istihbaratı hizmeti dahil edilebilir.*

***Mevcut durumda* ANEMON bünyesinde daha önceki bütçe görüşmelerinde SIEM yatırımlarının planlanmadığı görülmüştür.**

EYLEM PLANI:
Konu ile ilgili çalışılacak danışman kuruma ya da iç kaynaklara karar verilmesi gerekmektedir.

SIEM'in 7/24 sürdürülmesi gereksinimi belirli bir donanım ya da çalışan kaynağı gerektirebilir. Eğer uygulama bulut tabanlı sağlanırsa bu maliyet önemli ölçüde düşecektir. Bu karar Şirket tarafından verilmelidir. SIEM yatırımının **ANEMON** *2020 bütçe görüşmelerinde yeniden gündeme getirilmesi ve yol haritasına dahil edilmesi önerilmektedir.*

Dış kaynak ile çalışılmaya karar verilmesi halinde ihtiyaçları yansıtan hizmet seviyelerinin belirlenmelidir.

G	R04	C	Yetki Matrisi

Yetki Matrisi; verinin bulunduğu mecraları belirleyen ve bu kaynaklara erişimi detaylandırarak kontrol altına alan yetki-erişim haritasıdır.

Mevcut durumdaki tespitimiz **ANEMON bünyesinde sadece File Server için bir dokümantasyonun olduğu yönündedir. Bunun CRM ve ERP yazılımları için de zamanla oluşturulması gerekliliği aksiyon olarak karşılıklı istişare edilmiştir.**

Önerimiz periyodik aralıklarla yetki denetimlerinin gerçekleştirilmesi ve erişim ayrıcalık ve haklarının güncellenmesidir.

EYLEM PLANI:
IT ve Teknik İşler Birimi tarafından yetki matrisinin görsel (diyagram) formatta erişilebilir halde muhafaza edilmesi ve bu matrisin diğer önemli teknik tedbirler başlıkları altında bahsi geçen DLP, SIEM, firewall gibi projelerde de temel teşkil edeceği unutulmamalıdır. Bu sebeple yetki matrisi her zaman güncel ve doğru olmalıdır.

G R05 C Mobile Device Management – MDM

Kurumsal mobil cihazların önemli bir tehdit oluşturduğu açıktır. Kaybolan cihazları bulma, kilitleme ve potansiyel olarak silme olanağı bulunmalıdır. Bu işlemi otomatikleştirmek riski minimalize edecektir. Teknoloji desteği sağlanması bir cihazın belirli bir sınırı aşması durumunda uyarılar verebilecek ve harekete geçebilecek bir geofencing yeteneği sunmaktadır. Bu özellik seyahat eden çalışanlar için kontrol noktası olabilir. Masaüstü bilgisayarların kontrolünden çok daha kritik olan mobil aygıtların kontrolüdür.

***Mevcut durumda* ANEMON bünyesinde MDM çözümü olarak Manage Engine vb. bir çözüm mevcut değildir.**

EYLEM PLANI:

MDM konusu ilerleyen dönemde global IT yönetim birimi ile istişare edilerek yatırım planlamasına dahil edilmelidir.

G	R06	C	Mobile Device Security – MDS

Kurumsal mobil cihazların bir tehdit olduğu açıktır. Son kullanıcı koruma platformları arasında en fazla hassas verinin işlendiği ve saldırı vektörlerinin yoğun olarak görüldüğü alan olduğu yapılan çalışmalarda görülmektedir. Mobil sistemler bağlandıkları ağlar ve çalıştıkları uygulamalar özelinde hassas bilgilerden yararlanmak için kullanılabilir bir çalışanın belgeleri, takvim randevuları, e-posta mesajları, metinleri ve ekleri bu kapsama girmektedir. Siber suçlular bir cihazın mikrofon ve kamerasını, kapalı kapılardaki toplantılarda casusluk yapmak ve daha sonra gizli bir uzak sunucuya kayıt gönderebilir.

Mevcut durumda ANEMONcbünyesinde MDS çözümü olarak etraflı bir konfigürasyon bulunmadığı tespit edilmiştir. Kullanıcıların, hassas veriler içerebilecek ANEMON sistemlerinde oturum açmakta kullandığı kullanıcı adlarını ve şifreleri bile yakalayabilirler. Bu itibarla tüm tehditlerin mobil cihazlar düzeyinde kontrolünün sağlanması ve etkilerinin düşürülmesi gerekmektedir.

EYLEM PLANI:

MDS konusu ilerleyen dönemde icra kurulu yönetim birimi ile istişare edilerek yatırım planlamasına dahil edilmelidir.

G R07 C Database Security

Database security *(Veri tabanı güvenliği)* bir veri tabanı veya veri tabanı yönetim yazılımını güvenli olmayan kullanım, kötü niyetli tehditlerden ve saldırılardan korumak ve güvence altına almak için kullanılan ortak önlemleri ve etkin raporlama süreçlerini belirtir.

Veri tabanı güvenliği, veri tabanlarının tüm yönleri ve bileşenleri üzerinde güvenliği kapsar ve uygular. Bunlar; veri tabanında saklanan veriler, veri tabanı sunucusu, veri tabanı yönetim sistemi (DBMS), diğer veri tabanı iş akışı uygulamaları vb. KVKK'ya uygun şekilde database üzerinde canlı ve offline olarak saklanması için gerekli güvenli ortamın sağlanması beklenmektedir.

Mevcut durumda ANEMON 'da bu alt yapı sağlanmıştır.

EYLEM PLANI:
Database Security için ilgili yetkilendirmeler sağlanmalıdır.

Databaseler üzerinde gerçekleşen hareketleri sürekli olarak izlenmesi ve kontrolünün sağlanması gerekmektedir. Bu doğrultuda ilerleyen süreçlerde gerekirse veri tabanı yönetim ve raporlama yazılımları için bir yatırım planlaması yol haritasına dahil edilmelidir.

G R08 C User Behavior Analytics (UBA)

Kurumlarda yaşanan hukuki uyum ihlallerinin büyük bir çoğunluğunun kaynağı güvenilen ve kurum tarafından oluşturulmuş güvenilen hesaplar üzerinden gerçekleşmektedir. User Behavior Analytics kurum bağlı sistemlerinde yaşanabilecek güvenlik anormalliklerinin tespitini sağlar.

Kurum sisteminde bulunan varlıkların *(örneğin, kullanıcılar, aygıtlar, sunucular, uygulamalar vb.)* algoritmik yaklaşımda risk tabanında sapmalarını izlemek ve gerekli aksiyonların tespit edilmesini mümkün kılar. SIEM çözümleri günlük toplama ve korelasyona yardımcı olsa da saldırgan konumundaki varlıkların ihlal niteliğindeki aktivite tutarlılıkları desteklenen teknologiler ile sağlanmalıdır.

***Mevcut durumda* ANEMON bünyesinde mevcut herhangi bir UBA çözümünün bulunmadığı tespit edilmiştir.**

EYLEM PLANI:
Saldırgan konumundaki varlıkların ihlal niteliğindeki aktivitelerini tespit edebilen bu üst nitelikli çağdaş teknolojiler bugün olmasa da ilerleyen zamanlarda mutlaka Şirket envanterine dahil edilmelidir.

Tehditlerin daha etkili kaynaklarının Şirket içinden geldiği göz önünde bulundurulduğunda büyük bir zarara uğramamak için UBA ve eşdeğer yazılımlar önemli tavsiyelerimizden biri olacaktır.

G	R09	C	Server Encryption

Kişisel verilerin bulunduğu serverların encryption yöntemleri ile güvenliği saklama ve gerekli support hallerinde içeriğin erişilemeyecek ve güvenli halde paylaşılması hususlarını kapsamaktadır.

Mevcut durumda ANEMON bünyesinde Microsoft SQL server yazılımının kullanıldığı tespit edilmiş ve SQL server'ın ek şifreleme olmadan *default* özellikleriyle kullanıldığı gözlemlenmiştir KVKK teknik tedbirleri kapsamında disk şifreleme tavsiye edilen bir yöntemdir. Ancak bu yöntemin network performansında ciddi bir düşüşe neden olması da kaçınılmazdır. Dolayısıyla bu tedbirin sağlanması önerilmekle birlikte performans ve güvenlik arasındaki denge network administrator planlamasıyla ayarlanmalıdır. Ayrıca yine sistemde kullanılan Oracle tabanlı yazılımlar için arayüz olan Oracle'ın web tabanlı dashboard'u mevcut olmakla beraber bu altyapı ANEMON yeterli güvenlik ve performans yeterliliğini karşılamaktadır.

EYLEM PLANI:
Bu tedbirin sağlanması önerilmekle birlikte performans ve güvenlik arasındaki denge network administrator planlamasıyla tesis edilmdlidir.

G	R[10]	C	Disc Encryption (Full Enc. / Folder Enc.)

Laptop, PC ve taşınabilir cihazların disk şifrelemesi (disc encryption) olmaması hali cihazlara yetkisiz erişimlerin, kişisel verilerin ve/veya kuruma özel bilgilerin ifşa olmasının en yaygın sebebidir. Bu riski azaltmak için laptop, PC ve taşınabilir cihazları şifreleyen yazılımlar kullanılmalıdır. *Disk encryption yazılımları önemli ve öncelikli bir aksiyon olarak KVKK teknik tedbirlerinin başlıcalarındandır.*

***Mevcut durumda* ANEMON bünyesinde disc encryption korumasının Microsoft 'un Bitlocker uygulaması ile sağlandığı tespit edilmiştir.**

EYLEM PLANI:

Laptop, PC ve taşınabilir cihazların disk şifrelemesi olmaması hali cihazlara yetkisiz erişimlerin, kişisel verilerin ve/veya kuruma özel bilgilerin ifşa olmasının en yaygın sebebidir.

Bu riski azaltmak için laptop, PC ve taşınabilir cihazlar **ANEMON** *bünyesinde full disc encryption seviyesinde koruma altındadır. Bu konuda ekstra bir aksiyona gerek yoktur.*

G R11 C Merkezi Kimlik ve Erişim Yönetimi

Erişimler kurum iç ağından olabildiği gibi dış ağlar üzerinden de olabilmektedir. Bu erişimler için ihtiyaç duyulan kullanıcı ve kimlik bilgileri oluşturulduktan sonra yetkili olunan işlemler net bir şekilde belirlenmelidir. Yapılan her erişimin kendine has riskleri mevcut olduğundan, yapılacak risk değerlendirmesine göre süreçler iyileştirilerek, verilen kimlikler ve bu kimliklere ait yetkiler iş birimleri tarafından belirlenmiş süreler ve kapsamlarla sınırlandırılmalıdır.

ANEMON bünyesinde mevcut yapıda Active Directory kurulu ve kullanılmakta OLMADIĞI için Konfigürasyon bakımından uluslar arası standartlar karşılanamamakta ve arttırılmış bir kimlik ve erişim yönetimi yapısı oluşamamaktadır. Bu seviyede kurulum ve uygulama tavsiye edilmektedir.

EYLEM PLANI:

Tüm organiasyonun ve operasyonel kaynakların tek bir merkezden yönetimi sağlayabilecek bir Active Directory yapılanması planlaması önemli bir aksiyon olarak tavsiye edilmektedir.

G	R12	C	Sızma Testi

Siber güvenlik denetimi gerçekleştirilirken her bir test başlığı kapsamında saptanan açıklık ve bulgular, ayrı ayrı değerlendirilmenin yanında, bir araya geldiklerinde oluşturabilecekleri riskler ve açıklıklar açısından da değerlendirilir. Bu birlikte değerlendirme sonucu ortaya çıkan yeni açıklar ve bulgular da raporlanır. Bulgu önem dereceleri belirlenirken varlığın değeri dikkate alınmaz. Varlık değerlendirmesi yapmak ve varlıkların önem derecelerine göre aksiyon almak kurumun sorumluluğundadır.

ANEMON düzenli (1 yıl) aralıklarla sızma testlerini Merkez IT birimi vasıtası ile yapmaktadır.

EYLEM PLANI:

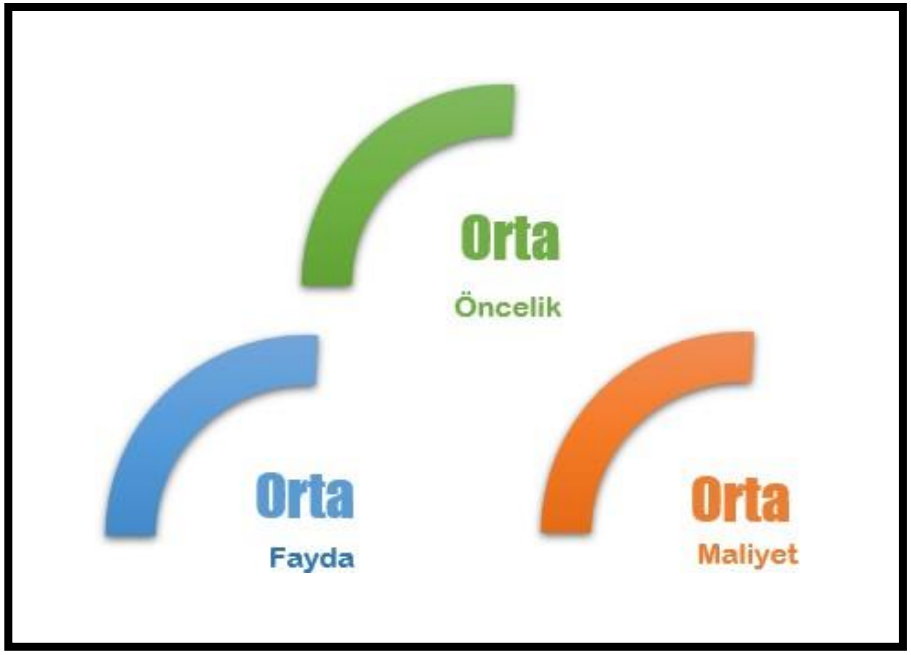
Gerçekleştirilen sızma testi kurum güvenlik zafiyetlerinin tespit edilmesi ve bu operasyon sonunda ortaya çıkan bulgu ve çıktıları göz önünde bulundurarak önleyici ve düzeltici aksiyonların alınması gereklidir.

IT ve Teknik İşler Birimi sızma testi projesinde yönetişim konusunda iş birimlerine destek sağlayacaktır. Ancak, projenin çıktılarına istinaden sürecin uygulanabilirliği iş birimlerinin sorumluluğundadır.

G	R13	C	Yedekleme

Mevcut durumda ANEMON bünyesinde yedekleme için Network NAS uygulaması kullanılıyor. Yedekleme planı olarak günlük full yedek alınıyor. Hem lokalde hem de TR'de bir bulut sağlayıcıda günlük, haftalık, aylık yedekler tutuluyor.

Kullanıcı bilgisayarları *(pc ve laptop)* kurulumları ve yedeklemesi için manual olarak periyodik kontrollerle sağlanmaktadır.



G	R14	C	Altyapı Güvenliği

Anti-virüs ve Zararlı Yazılımlardan Koruma; Bilgisayar virüsleri, truva atları, casus yazılım ve reklam yazılımları dahil fakat bunlarla sınırlı olmamak üzere engelleme, zamanında tespit ve zararlı yazılımlardan kurtulma süreçlerini sağlayan yazılım ve donanım konfigürasyonunu kapsar.

Ağ ve Uygulama Güvenlik Duvarı; Host, servisler ve uygulamalara yetkisiz erişimi engellemek için kısıtlı ve özel ağdan erişim kontrolleri oluşturmak, güncel tehditler ve istismarlara dayanan web uygulama saldırılarını tespit etme ve bloklama süreçlerini kapsar.

Ağ Erişim Kontrol; Kimliklendirme, cihaz doğrulama, cihazların güvenlik politika uyumluluklarını kontrol etme ve izin vermeden önce cihaz iyileştirmeyle entegre olarak şirket ağına erişim kontrolü yapma süreçlerini kapsar.

Uzaktan Erişim Kontrolü; Kurumsal ağa uzaktan yapılacak erişimlerde güvenlik ihtiyaçlarının belirlenmesi ve kontrollerin oluşturulması süreçlerini kapsar.

Mevcut durumda **ANEMON erişim yönetimi *(yetkilendirme ve engelleme)* ve ağ güvenliği başlıkları bakımından KVKK teknik tedbirler rehberindeki yetkinlik seviyesini karşılamaktadır. Yine de bu cihaz ve uygulamalardaki konfigürasyon yetki matrisi temel alınarak ve güncelliği teyit edilerek her zaman kontrol altında tutulmalıdır.**

EYLEM PLANI:

Konuyla ilgili prosedür hazırlanmalı ve yayınlanmalıdır. Eğer güvenlik seviyesi arttırılmak istenirse internet çıkış noktasına ve kritik ağ segmentleri giriş noktalarına ağ durum denetimi yapan (statefull inspection) güvenlik duvarları konumlandırılmalıdır. (Örn; üçüncü parti bağlantı noktaları, PCI ağ segmentleri)

Güvenlik duvarı kuralları için gözden geçirme ve onay süreci oluşturulmalıdır.

Güvenlik politikası ile uyumlu olmayan cihazların ağ bağlantısı reddedilmelidir ve karantina alanı, misafir ağ gibi kısıtlı bir alana yönlendirilmelidir.

G	R15	C	Hukuksal Metinlerin Dijital Yönetimi

Çalışanlarla ilgili adli yazışmalar veya takipler, tedarikçilerle / müşterilerle yapılmış sözleşmeler, sigorta poliçeleri, hukuk işlerinin yönetilmesi için düzenlenen vekaletname ve noter belge örnekleri gibi hukuksal metinlerin güvenliği KVKK bakımından son derece hassasiyet arz etmektedir.

Bunların korunması idari tedbirlerle olduğu kadar teknik tedbirlerle de desteklenmelidir.

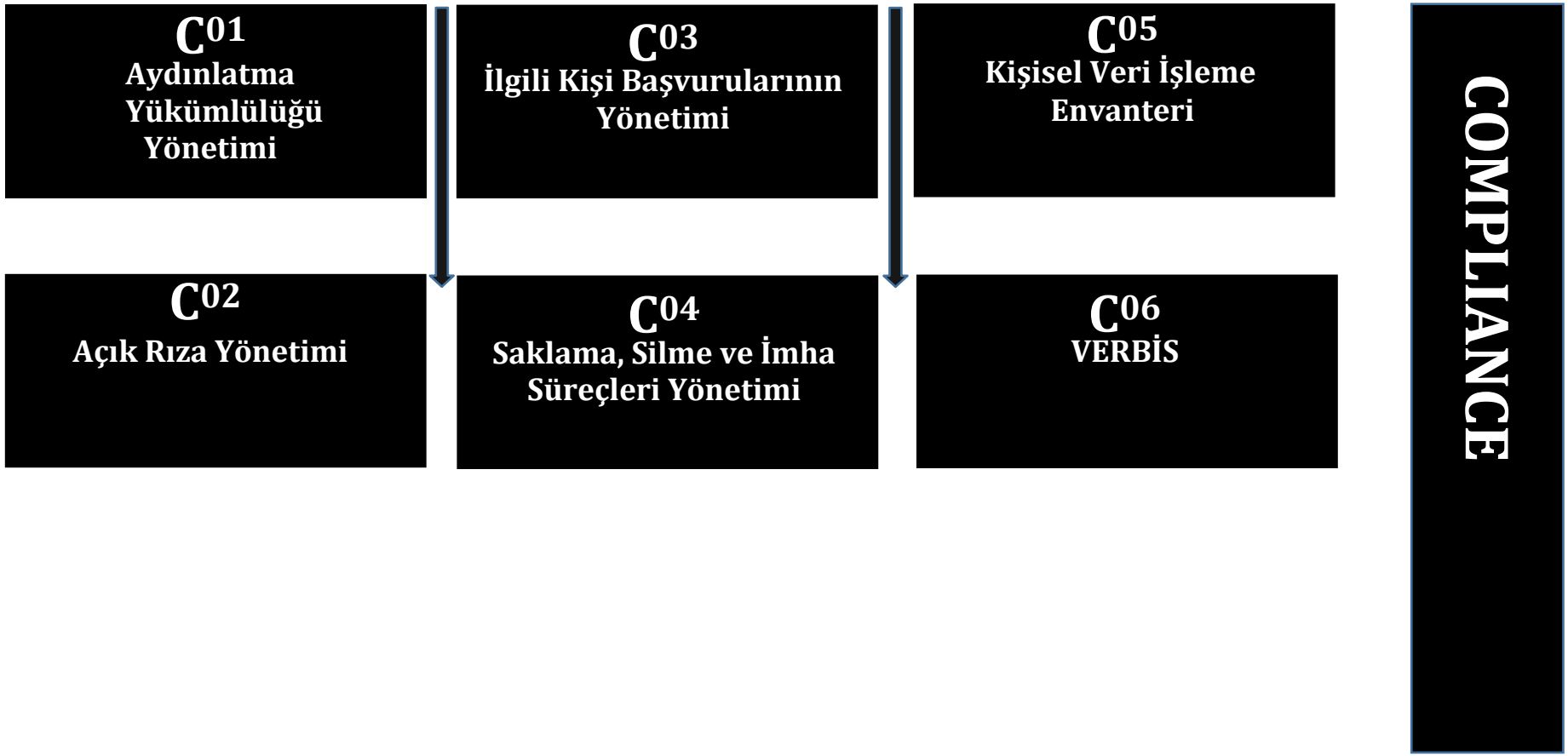
EYLEM PLANI:

Kişisel veri işleme envanterleri aracılığı ile tespit edilen süreçlere ilişkin Kanun'a uyum kapsamında ilgili gerçek kişilerden dijital formlar aracılığıyla toplanarak yönetilmesi.

Taraflara iletilmesi gereken hazırlanmış hukuki metinlerin (aydınlatma, açık rıza, şikâyet, talep vb.) bir uygulama yardımı ile kurum dijital veri yapılarına adapte edilmesi.

Özel nitelikli kişisel veri ihtiva etme potansiyeli bulunan bu tip belgeler Kurum'a giriş noktasından itibaren kontrol altında olmalı; ilgilisi ve yetkilisi dışında bir temasa maruz kalmamalıdır.

UYUMLULUK ANALİZİ PROJE KARTLARI



Aydınlatma Yükümlülüğünün Yönetimi

"Aydınlatma yükümlülüğünün yerine getirilmesi sürecinin kurgulanması" önemli bir proje çıktısı olacaktır. Aydınlatma yükümlülüğü açık rıza şartından farklı olarak rıza alınmasına gerek olmayan hallerde dahi yerine getirilmesi gereken bir yükümlülüktür. Dolayısıyla verinin sahibi rıza gösterse dahi aydınlatma yapmak veri sorumlusunun yükümlülükleri arasındadır.

Veri sorumlusu sıfatıyla hareket eden **ANEMON** 'un kişisel veri işleme faaliyetlerine ilişkin olarak aydınlatma yükümlülüğünü yerine getirilebilmesi amacıyla hazırlanan aydınlatma metinleri işbu Rapor teslim tarihi itibarıyla ilgili kanallarda uygulamaya alınmıştır. Böylelikle, **ANEMON** bu yükümlülüğün ihlali halinde yaptırımı 300.000 TL'ye kadar varabilecek idari para cezası riskini bertaraf ederek aydınlatma yükümlülüğünü yerine getirmiş olacaktır.

EYLEM PLANI:

Kişisel Veri İşleme Envanteri'nden yararlanarak tespit edilen veri giriş kanallarında aydınlatma yükümlülüğünün yerine getirilmesine ilişkin görev ve sorumlulukların belirlenmesi,

Kişisel verilerin işlenmesine ilişkin süreçler kapsamında gerçekleşen değişikliklere göre aydınlatma metinlerinin güncellenebilmesini sağlayacak gerekli takip ve onay mekanizmalarının oluşturulması.

Açık Rıza Yönetimi

Açık rıza beyanı alınması gereken süreçlerin yönetimi proje çıktısı olarak tespit edilmiştir. Kanun'da öngörülen istisnalar hariç olmak üzere, kişisel veriler ancak ilgili kişilerin açık rızası ile işlenebileceğinden, **ANEMON** tarafından yürütülen kişisel veri işleme faaliyetleri kapsamında açık rıza gereken süreçlerde, Kanun'da öngörülen şartları taşıyan nitelikte açık rıza temini, elde edilen açık rıza beyanlarının saklanması ve gerektiğinde revize edilmesi sağlanmıştır.

Bu itibarla, veri sorumlusu sıfatıyla hareket eden **ANEMON** 'un veri işleme faaliyetlerine ilişkin olarak açık rıza alma yükümlülüğünü yerine getirilebilmesi amacıyla hazırlanan açık rıza beyanları işbu Rapor teslim tarihi itibarıyla ilgili kanallarda uygulamaya alınmıştır.

EYLEM PLANI:

Kişisel Veri İşleme Envanteri'nden yararlanarak süreç bazında açık rıza teminine ilişkin plan, görev ve sorumlulukların belirlenmesi.

Kişisel Veri İşleme Envanteri'nden yararlanarak elde edilen açık rızaların toplanması ve iyi uygulama örneği olarak belirli aralıklarla güncellenmesi, ilgili kişinin talebi halinde geri alınmasının sağlanması.

Kişisel Veri İşleme Envanteri'nden yararlanarak Kanun'un yürürlüğe girmesinden önce elde edilen veriler için açık rıza temini süreçlerinin kurgulanması.

G R C03 İlgili Kişi Başvurularının Yönetimi

İlgili kişilerin başvurularının yönetimi de önemli bir proje kalemi ve kanuni yükümlülüktür.

İlgili kişiler, Kanun'un uygulanmasıyla ilgili taleplerini veri sorumlusu sıfatıyla hareket eden **ANEMON**'a ilettiğinde, **ANEMON** talebin niteliğine göre ve en geç 30 gün içerisinde ilgili talebi sonuçlandırmak zorundadır.

Bu nedenle, ilgili kişilerin başvurularına ilişkin süreçlerin kurgulanarak uygulamaya konulması gerekmektedir. Tarafımızca daha önce hazırlanmış ve teslim edilmiş KVKK Uyumluluk Projesi İdari Rapor ve ilgili prosedürlerde bu süreç tesis ve temin edilmiştir.

EYLEM PLANI:
İlgili kişilerin Kanun'un uygulanmasına ilişkin başvurularının alınmasından itibaren cevaplanarak tamamlanması sürecinin kurgulanması, yönetimi ve denetimi (başvuru yolu, başvuru metinleri, ilgili kişilerin başvuru prosedürü hakkında bilgilendirilmesi ve başvuru yapan kişinin ilgili verinin sahibi olup olmadığının kontrolüne ilişkin yöntemlerin belirlenmesi vb.).

Başvuruların toplandığı adımdan itibaren başlayan 30 günlük sayacın tüm süreçlerinin takip edilebileceği ve raporlanabileceği bir iş akış takip sisteminin kurulması veya var olan bir akış sistemine sürecin entegre edilmesi.

G	R	C⁰⁴

Saklama, Silme ve İmha Süreçleri Yönetimi

Verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin süreçlerin yönetimi proje çıktısı olarak tespit edilmiştir. Kişisel veriler, Kanun, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik ve ilgili diğer mevzuata uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde re'sen veya ilgili kişinin talebi üzerine silinmek, yok edilmek veya anonim hale getirilmek zorundadır.

Veri sorumluları gerçekleştirmekte oldukları saklama ve imha faaliyetlerine ilişkin iş ve işlemler konusunda usul ve esasları belirlemek amacıyla Veri Saklama ve İmha Politikası oluşturmalıdır. Veri sorumlularının çalışanları, çalışan adayları, ziyaretçileri veya diğer üçüncü kişilere ait kişisel verilerin işlendiği tüm kayıt ortamları ve kişisel veri işlenmesine yönelik yürütülen tüm faaliyetlerinde oluşturdukları bu politika uygulanacaktır.

Bu nedenle, veri sorumlusu sıfatıyla hareket eden ANEMON ’un öncelikle işlediği her bir verinin ilgili mevzuat veya işleme amacını göz önünde bulundurarak saklama süresi belirlemiş, tespit edilen sürelerin sona ermesi halinde ise, sakladığı verileri silmesi, yok etmesi veya anonim hale getirilme yükümlülükleri bakımından önlemlerini almıştır. Böylelikle, ANEMON ihlali halinde yaptırımı 1 yıldan 2 yıla kadar hapis cezası olan söz konusu yükümlülüğünü yerine getirmiş ve veri güvenliğini sağlamaya yönelik önemli bir yükümlülüğü takip ve kontrol altında tutmaktadır.

EYLEM PLANI:

Veri işleme faaliyetinin gerçekleştirildiği her bir süreç özelinde, ilgili verilerin saklanma sürelerinin tespit edilmesi ve **ANEMON** nezdinde *tek tip uygulamanın sağlanması amacıyla belirlenen sürelerin fiziki veya elektronik ortama kaydedilerek saklanması.*

Tespit edilen sürelerin dolması üzerine, verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin gerekli işlemlerin yapılması ve bununla ilgili prosedürlerin belirlenmesi ve kaydedilmesi.

Uyuşmazlık durumunda ileride delil olarak kullanılmak üzere, ilgili verilerin silindiği, yok edildiği veya anonim hale getirildiğine ilişkin gerekli kayıtların alınıp saklanması (log ya da tutanak).

G	R	C05

Kişisel Veri İşleme Envanteri

Veri sorumluları için VERBİS'e kayıt yükümlülüğünün getirdiği öncelikli görev her şirketin kendine ait bir Veri Envanteri oluşturmasıdır. Kişisel Veri Envanteri, işleme amaçları, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirilerek oluşturulan, kişisel verilerin işlendikleri amaçlar için gerekli olan azami sürelerin ve yabancı ülkelere aktarımı öngörülen kişisel veri varsa belirtildiği ve veri güvenliğine ilişkin alınan idari ve teknik tedbirlerin yer aldığı bir envanterdir. Bu envanterin oluşturulması ve kaydı ile amaçlanan Sicil vasıtasıyla veri sorumlusu ve yaptığı kişisel veri işleme faaliyetlerine ilişkin herkesin sağlıklı ve şeffaf bilgiye erişiminin sağlanmasıdır.

EYLEM PLANI:

Kişisel Veri İşleme Envanterleri'nin manuel takibinden kaynaklı hata ve gecikmelerin giderilmesi için; proje kapsamında oluşturulan envanter çalışmasının bir veri tabanı üzerinden takip edilebilmesi, güncellenebilmesi ve gerekli raporların alabilmesi için gerekli olan teknik sistem ve yazılım geliştirilmesi ya da tedarik edilmesi.

Denetim, veri sahibi başvurusu, VERBİS süreçlerinin yönetimi ve diğer kişisel veri işleme faaliyetleri kapsamında kişisel veri işleme envanterinde süreç olarak yer alması.

G	R	C⁰⁶

Veri Sorumluları Sicil Bilgi Sistemi (VERBİS)

Uyumluluk sürecinde bir diğer önemli yükümlülük Veri Sorumluları Sicil Bilgi Sistemi'ne **("VERBİS")** kayıt zorunluluğu olup, bunun için tanınan süre 30 Haziran 2020 tarihinde son bulmuştur. Kural olarak her gerçek ve tüzel kişi için bahsi geçen kayıt zorunlu olmakla birlikte Kişisel Verileri Koruma Kurulu 19 Temmuz 2018 tarihli ve yayınladığı diğer kararları ile veri sorumlularının VERBİS'e kayıt yükümlülüklerini, kayıt sürelerini ve muaf olma kriterlerini belirlemiştir.

Veri sorumlusu olarak ANEMON *"yıllık çalışan sayısı 50'den çok veya yıllık mali bilanço toplamı 25 milyon TL'den fazla olan gerçek ve tüzel kişi"* kriterini karşıladığından ötürü VERBİS kayıt yükümlülüğü altındadır. Tarafımızca ANEMON adına VERBİS başvuruları yapılmış, veri sorumlusu ve irtibat kişisi kayıtları gerçekleştirilerek resmi sicil envanter girişleri ANEMON KVKK Komitesi ile koordineli bir şekilde gerçekleştirilmiştir.

EYLEM PLANI:

VERBİS için gereken aşağıdaki eylemler gerçekleştirilmiştir:
- *Veri Envanteri*
- *Veri Saklama ve İmha Politikası*
- *İrtibat kişisinin belirlenmesi ve kaydı*

Yine de eğer bu üç unsurda bir değişiklik söz konusu olursa ilgili belgeler güncellenmeli, üçüncü unsur olan irtibat kişisi için bir değişiklik söz konusu olursa Kişisel Verileri Koruma Kurumu ile gerekli irtibat sağlanarak 7 gün içinde bu kayıt güncellenmelidir.