...making excellence a habit.™

Gizlilik düzenlemeleri

ISO/IEC 27701'in rolüne genel bakış

Hazırlayan: Kieran McDonagh, Riskscape Law Ltd

Teknik inceleme

İçindekiler

Giriş	3
Avrupa gizlilik mevzuatı	4
ISO/IEC 27701'in rolü	4
Standardın avantajları	5
Temel kavramlar	7
Gizlilik düzenlemelerine genel bakış	10
e-Gizlilik yönetmeliğinden kaynaklanan sorunlar - AdTech iş modeli	11
Büyük veri sayfalarını işleyenlerin rekabet hukukuyla ilgili karşılaştığı sorunlar	12
Çevrimiçi gönderilen kişisel verilerin doğurabileceği zararlar	12
Gizlilik ve bilgi güvenliği standartlarının uygulanması	13
Gizlilik yönetimi	13
Sonuç	14

Giriş

Bireylere ait kişisel verilerin gizliliği günümüzde büyük önem taşıyan bir konu haline gelmiştir. Kuruluşların müşterilere, çalışanlara, ziyaretçilere ve komşulara ait kişisel bilgileri nasıl yönetip işleyeceğini dikkatli bir şekilde değerlendirmesi gerekiyor. Ancak birçok kuruluş bunu yapmakta zorlanıyor. Mayıs 2018'de yürürlüğe giren GDPR (Genel Veri Koruma Yönetmeliği), AB vatandaşlarının kişisel verilerini işleyen tüm kuruluşların, nerede mukim olursa olsunlar, GDPR'ye uygun hareket etmesini zorunlu kılmıştır. AB'nin dışında en az 132 ülkede daha artık gizlilik yasaları uygulanmaktadır. Gizlilik yasaları bulunan ülkeler arasında kişisel veri aktarımı gerçekleştiren kuruluşlar, gizliliği korumaya yönelik kontrol önlemlerini tasarlarken geçerli her bir yasayı dikkate almak durumundadır.

Bu yasalara uygunluğu destekleyecek kontrol önlemlerinin uygulanması ve izlenmesi karmaşık bir hal alabiliyor. Söz konusu süreci daha yönetilebilir kılmak adına standartların uygulamaya konulması, kuruluşların mevzuata uygunluğu sağlama konusunda daha emin adımlar atmasına yardımcı olabilir. Bu gibi standartlardan biri de, kuruluşların mevcut ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemlerinin (ISMS) kapsamını, gizlilik gerekliliklerini de ele alacak şekilde genişletmesine imkan veren uluslararası kabul gören bir standart olan ISO/IEC 27701'dir.

Bu teknik incelemede gizlilikle ilgili düzenlemelere ve ISO/IEC 27701'in rolüne dair bir genel bakış sunulmakta ve standardın işletmeler ve tüketiciler açısından ne anlama geldiği ele alınmaktadır.

Avrupa gizlilik mevzuatı

Milyonlarca Avrupalı tüketicinin kişisel verileri, 25 Mayıs 2018'den beri GDPR ile korunmaktadır. Kişisel verileri işleyen tüm kuruluşlar, hangi boyutta olursa olsunlar, GDPR'ye veya GDPR'yi içine alan yerel yasalara uymalıdır. Buna göre, örneğin, Birleşik Krallık'ta bu gibi kuruluşların 2018 tarihli Veri Koruma Kanunu'na (DPA 2018) uyması gerekir.

2009'da Lizbon Antlaşması yoluyla yürürlüğe giren AB Temel Haklar Şartı bireylerin gizlilik hakkını içermektedir. GDPR, bu gizlilik hakkı üzerine inşa edilmiş olduğundan, bireylerin kişisel verilerinin toplanmasını, analiz edilmesini, paylaşılmasını, depolanmasını ve silinmesini içeren faaliyetlerde (tüm bu faaliyetler toplu olarak "işleme" faaliyeti olarak anılır) gizliliğin dikkate alınmasını ve korunmasını gerektirmektedir. GDPR, kişisel verilerin işlenmesinde aşağıdaki şartların yerine getirilmesini öngören bir dizi ilke içermektedir:

- kişisel veriler yasalara uygun ve ilgili birey için adil ve şeffaf bir şekilde işlenmelidir
- kişisel veriler belirli amaçlar doğrultusunda toplanmalı ve başka amaçlarla yeniden kullanılmamalıdır
- kişisel veri toplama ve işleme faaliyetleri en aza indirilmelidir
- kişisel veriler güncel tutulmalıdır
- kişisel veriler mümkün olan en kısa süre boyunca depolanmalıdır
- kişisel veriler yetkisiz işlemeye ve kayıp, imha veya zarara karşı korunmalıdır

GDPR, bireylerin kişisel verilerini korumak için uygulanması gereken denetimlerin türlerini belirlemektedir. Kişisel verilerin nasıl işlendiği incelenirken, GDPR söz konusu işlemenin kişisel verileri işlenen bireylerin hak ve özgürlükleri açısından yüksek bir risk teşkil edip etmediğinin değerlendirilerek belirlenmesini gerektirir. Bu değerlendirme, kişisel verilerin işlendiği birçok farklı koşul altında uygulanmalıdır. Bazı kuruluşlar bu riskleri değerlendirmekte güçlük çekmiş ve düzenleyici kurumlara başvurarak değerlendirmenin yürütülmesi konusunda tavsiye ve kılavuzluk talep etmiştir.

ISO/IEC 27701'in rolü

ISO/IEC 27701 standardı, ISO/IEC 27001 BGYS'nin (ISMS) kapsamını gizlilik gerekliliklerini de içine alacak şekilde genişletmektedir. Birçok kuruluşta zaten bir ISO/IEC 27001 BGYS (ISMS) bulunuyor olması, gerekli zeminin zaten hazır olması nedeniyle bir Gizlilik Bilgisi (Kişisel Veri) Yönetim Sistemi (PIMS/KVYS) kurma işleminin karmaşıklığını azaltmaktadır.
ISO/IEC 27001 konusunda bilgi sahibi kuruluşlar, BGYS'lerini gizlilik gerekliliklerini içine alacak ve GDPR'ye ve diğer gizlilik yasalarına uygunluklarını destekleyecek şekilde genişletebilir ve kişisel veri yönetimine bağlılıklarını sergileyebilirler.

Standartta kişisel veriler veya Kişiyi Tanımlamak için Kullanılan Bilgiler (PII) ile ilgili sistematik ve şeffaf bir yönetim uygulanmasını sağlamak için gerekli denetimleri tanımlanmaktadır. Kuruluşun PII denetleyicisi veya işlemcisi rolünde hareket ettiği durumlarda gerekli olan denetimleri belirlemektedir.

Standarttaki denetimler, PII toplama, analiz, paylaşım, depolama ve silme sürecini baştan sona kapsamaktadır. GDPR gerekliliğine uygun olarak, bu denetimlerin odak noktasında PII'sı işlenen birey bulunur.

Standardın avantajları

Global tutarlılık

Kuruluşlar genellikle birden çok ülkede faaliyet gösterir ve dolayısıyla farklı yargı yetki bölgelerinde geçerli olan birçok gizlilik ve bilgi güvenliği gerekliliğine tabidir. Bir kuruluş, uluslararası kabul gören bir standardı kullanarak tüm gerekllikleri bir araya getirebilir. Bu durumda, uygunluğu elde etmek ve korumak için yalnızca tek bir eylem kümesini takip etmesi yeterli olur. Bu özellikle kuruluşların sınır ötesi PII aktarımı yaptığı ve sınırın karşı tarafında farklı yasaların ve denetim gerekliliklerinin bulunduğu durumlarda önem arz eder.

Paydaş yönetimi

Bir standart aynı zamanda kuruluşun Yönetim Kurulu veya müşteri temsilcileri gibi paydaşları tarafından belirlenen ek gerekliliklerin dahil edilmesine imkan veren bir yapı sağlayabilir.

Gizlilik ve bilgi güvenliği uygunluğuna yönelik en iyi uygulama standardına dayalı standart hale getirilmiş bir yaklaşım, uygunluk programı için net olarak belirlenmiş bir başlangıç noktası, orta nokta ve bitiş noktası sağlar. Bir standardın gerekliliklerinin karşılanması, uygunluğun elde edilmesine veya korunmasına ilişkin iş gerekçesini desteklemek üzere kullanılabilir ve konunun üst yönetimin dikkatine daha somut bir şekilde sunulmasına yardımcı olabilir. Güçlü paydaş desteği bu gibi bir programın başarıya ulaştırılmasında önemli bir rol oynar.

Program yönetimi

Herhangi bir sermaye harcamasının resmi bir proje üzerinden yönetilmesinde ısrar eden bir kuruluş, program yönetimi için bir standardı çerçeve olarak kullanabilir. Böylece, hem değişiklik hem de "olağan iş" faaliyetlerinin risk değerlendirme, azaltma ve izleme faaliyetlerini dahil edebilir.

Programlar birlikte gerçek manada değer yaratabilecek gerekllikleri ve proje hedeflerini tanımlamak için genellikle resmi bir süreç kullanır. Bir standart tam da bunun yapılmasına yönelik bir yapı sağlar ve bir harici veya dahili değerlendirmeyle bir arada kullanıldığında, uygunluk faaliyetlerinin koordinasyonu açısından sıkı bir çerçeve sağlar. Bu durum, dikkat dağınıklığını ve tali sorunlara takılıp kalmayı önler, uygunluğun elde edilmesine ve korunmasına odaklanılmasını sağlar.

Program yönetimi disiplininin bir parçası olarak bir standardın kullanılması, farklı departmanların, coğrafyaların ve teknik fonksiyonların tek bir şeffaf gereklilik kümesi üzerinde birlikte çalışmasına yardımcı olabilir. Bu, sınır ötesi veri aktarımlarının birden fazla ülkede denetlenmesi gereken durumlarda önem arz eder.

Ayrıca, bir proje teslim yaklaşımı kullanıldığında ilerleme durumunu üst yönetime, uygunluğu elde etme ve koruma çalışmalarına güveni artıracak bir şekilde açıklamak için basit ölçümler kullanılabilir. Üst yönetime gizlilik ve bilgi güvenliği uygunluğu konusundaki ilerleme durumuna dair kolay anlaşılır bir genel bakış sunulması, GDPR gibi yeni yasalarla ilişkili yasal risklerin yönetimi açısından önemlidir. Uygunsuzluk durumunda milyonlar düzeyinde para cezaları kesildiği için bu üzerinde durulması gereken önemli bir husustur.

Dahili eğitim

Bir standart belgesi, uzman olmayan kişileri standardın teknik disiplini alanında eğitmek için de kullanılabilir. Aynı zamanda kuruluş genelinde farkındalık eğitimi sağlayan ve teknik personelin kendi alanında uzman kişiler olarak akredite edilmesini sağlayan eğitim programlarının yapılandırılmasına yardımcı olabilir. Bir kuruluş uygunluğu elde etmek istiyorsa gizlilik ve bilgi güvenliği denetimleri her personel, danışman, yüklenici, ziyaretçi ve üçüncü şahıs tarafından başarıyla uygulanmalı ve takip edilmelidir. Her grup kendi ihtiyaçları doğrultusunda özel eğitim programlarına ihtiyaç duyar. Grupların sorumluluklarının tam olarak farkında olmasını ve denetimleri etkin bir şekilde uygulamasını sağlamak için özel eğitim programları gereklidir. Bir standart, farklı gruplar genelinde ortak mesajlar ileten, kapsamlı eğitim programlarına olanak tanıyacak bir çerçeve sağlar.

Güvence

Bir standart ayrıca denetimlerin test edilmesine ve başarılı test sonuçlarını kullanarak gizlilik ve bilgi güvenliği konusunda güvence sağlanmasına yönelik bir çerçeve sunacak şekilde kullanılabilir. Standart, denetim hedeflerine dönüştürülebilecek gerekliliklerin tesis edilmesine yardımcı olur ve bir kuruluşun gizlilik ve bilgi güvenliği gerekliliklerine uygunluk için uygulamaya koyması gereken özel denetimlerin tanımlanmasına destek olabilir. Daha sonra dahili ve harici paydaşlara güvence sağlamak amacıyla denetimlerle ilgili testler planlanabilir, gerçekleştirilebilir ve raporlanabilir. Bir standart, bu iş akışının sistematik olarak düzenlenmesine ve üst yönetim hedeflerini karşılamak üzere bir proje olarak yönetilmesine imkan verir.

Kabul gören bir standarda uygunluğun elde edildiğini ve korunduğunu göstermek, düzenleyici kurumlar ve tedarik zincirinde yer alan tedarikçiler gibi dahili ve harici paydaşlara güvence verilmesine yardımcı olabilir. Her ikisi de bir kuruluşun gizlilik ve bilgi güvenliği gerekliliklerine uygunluğu ile ilgili güvence almakta ısrar edecektir ve tedarikçiler bileşen veya hizmet kabul etmeden önce buna ihtiyaç duyacaktır. Bu gereklilik, tedarik zinciri güvencesinin gün geçtikçe daha önemli bir parçası haline gelmektedir. Bir standart, hem üretim hem de tüketim yönündeki tedarik zinciri iş ortaklarının bilgi paylaşımı risklerini anlamasına olanak tanıyan başlangıç düzeyi denetimler sağlar ve bu iş ortaklarının kendi veri aktarımlarına ek denetimler uygulayarak tüm kalıntı riskleri azaltmasına olanak verir.

Proaktif yaklaşım

Ne kadar gizlilik ve bilgi güvenliği denetimi uygulanırsa uygulansın, kuruluşlar yine de veri ihlaliyle karşılaşma riski altında olacaktır. Bir kuruluşun bir standarda uygunluğu sağlamasına rağmen gizlilik veya bilgi güvenliği ihlaliyle karşılaştığı durumlarda, kuruluş en iyi uygulama standardına uymasına rağmen söz konusu ihlalle karşılaştıklarını iddia edebilir. Bunun tam tersi durumda ise standarda uygunluğu sağlamak için elinden geleni yaptığını gösteremez ve dolayısıyla risk altında kalır.

Bu gibi bir ihlal ilgili düzenleyicilere raporlanırken, kabul gören bir standarda uygunluğun sağlanmış olması, düzenleyicilere denetimlerin sistematik bir şekilde düzenlendiği ve ihlalin ardından kolaylıkla güçlendirilebileceği yönünde güvence sağlayabilir. Bir standarda uygunluğun sağlanmamış olması durumunda ise kuruluşlar olgun bir denetim ortamına sahip oldukları ve gizlilik ve bilgi güvenliği gerekliliklerini ciddiyetle ele aldıkları konusunda düzenleyicileri ikna etmede sorun yaşayabilir.

Bu gibi durumlarda düzenleyicilerle yapılan görüşmeler genellikle yaptırımları içermektedir. Kuruluş kabul gören bir standarda uygunluğunu, yaptırım veya para cezalarına karşı kendini savunurken hafifletici bir etken olarak gösterebilir. GDPR kapsamında çok ciddi meblağlarda (yıllık küresel cironun yüzde dördüne kadar) para cezaları kesilebileceği için kabul gören bir standarda uygunluğun sağlanması yönünde yatırım yapılması son derece kârlı bir karar olabilir.

Temel kavramlar

Gizlilik ve bilgi güvenliği gereklilikleriyle ilgili olarak kullanılan terimler, bu alanda yeni çalışmaya başlayan kişilere göz korkutucu gelebilir. Ancak, temel kavramların tanımlanması, uluslararası standartlar oluşturulurken yürütülen çalışmaların önemli bir parçasıdır. Dolayısıyla bu tanımlar yardımcı olarak kullanılabilir. Bazı tanımlar uygulayıcılar tarafından yaygın olarak kabul edilip kullanılırken, diğerleri ise bazen süresiz olarak tartışma konusu olmaktadır. Buna rağmen, standartlar uygulayıcıların denetimleri uygularken günlük işlerinde kullanabilecekleri temel kavramların uluslararası olarak kabul gören tanımlarını sunar. Gizlilik ve bilgi güvenliği alanındaki bir uygunluk programının gerektireceği temel kavramlardan pek çoğu ISO/IEC 27701 ve ilişkili standartlarda tanımlanmıştır. Bu temel kavramlardan bazıları aşağıda açıklanmaktadır.

Tanım: Kişiyi Tanımlamak için Kullanılan Bilgiler (PII)

ISO/IEC 27701:2019'da, bilgi güvenliğinin ve ilişkili denetimlerin ele alındığı ISO 2700x serisi standartlarda ortak olarak yer alan terminoloji kullanılmıştır. Bu standartta geçen Kişiyi Tanımlamak için Kullanılan Bilgiler (PII) terimi bir PII sahibi veya birey için güvenlik ve gizlilik sağlanırken korunması ve yönetilmesi gereken bilgi varlıklarını ifade eder.

PII, ISO/IEC 29100:2011 Bölüm 2.9'da, bir PII sahibini veya bireyi tanımlamak için tek başına veya başka bağlantılı bilgilerle birlikte kullanılabilecek bilgi olarak tanımlanmıştır. Bu terim daha çok tıbbi kayıtların ve diğer kişisel sağlık bilgilerinin korunmasını hedefleyen Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPPA) gibi ABD Federal Yasalarında görülmektedir. Dolayısıyla, örneğin, bir bireyin IP adresi tek başına PII sayılmaz. Ancak, bu bilginin IP tahsisi tablolarındaki adlar gibi başka bağlantılı bilgilerle bir araya getirilmesinin makul olarak mümkün olduğu durumlarda, bu bilgi PII sayılır.

Hassas PII terimi, ISO/IEC 29100:2011 Bölüm 2.26'da, bir PII sahibi veya birey ile ilgili en mahrem ayrıntılarla ilgili bilgiler içeren ya da açıklanması durumunda bireyi önemli derecede etkileyebilecek PII olarak tanımlanmıştır.

Tanım: Gizlilik

"Gizlilik", PII'nın "işlenmesi" üzerinde yeterli denetimler uygulandığında ortaya çıkacak nihai sonucu ifade eder. ISO/IEC 29100:2011 Bölüm 2.22'de bir gizlilik paydaşı, PII'nın işlenmesiyle ilgili bir karardan veya faaliyetten etkilenebilecek bir PII sahibi veya birey olarak tanımlanmaktadır. Dolayısıyla, gizlilik, PII'nın işlenmesi sonucunda PII sahiplerinin veya bireylerin maruz kalabileceği olumsuz etkilerin önlenmesi olarak tanımlanabilir.

GDPR'de gizlilik teriminin tanımı verilmemiş olsa da, 1. Maddede gizliliğin amacı, kişisel verilerin işlenmesiyle ilgili olarak bireylerin temel hak ve özgürlüklerinin korunması, özellikle de kişisel verilerinin korunmasını talep etme hakkı olarak ifade edilmiştir.

PII gizliliği ile ilgili risk, ISO/IEC 29100:2011 Bölüm 2.19'da bir olay, bu olayın meydana gelme olasılığı veya PII'nın gizliliği açısından doğuracağı sonuçlar hakkındaki bilgi açığının etkisi olarak tanımlanmıştır.

Gizlilik denetimleri terimi, ISO/IEC 29100:2011 Bölüm 2.14'te gizlilik risklerinin meydana gelme olasılığını azaltarak veya sonucunu hafifleterek bu riskleri gidermeye yönelik organizasyonel, fiziksel ve teknik önlemler olarak tanımlanmıştır.

Kişisel veri - AB terminolojisi

AB'de, "kişisel veri" terimi GDPR'de kullanılmıştır. "Kişisel veri", 4. Maddede makul araçlar kullanılarak bir bireyin kimliğinin tanımlanmasına olanak sağlayabilecek, söz konusu bireyle ilgili herhangi bir bilgi olarak tanımlanmıştır. Dolayısıyla, örneğin, adı açıklanmamış olsa bile bir bireyin IP adresi üzerinden kimliğinin tanımlanması, bu bilgiyi "kişisel veri" kılacaktır.

AB'de, GDPR'nin 5. Maddesinde özel kişisel veri kategorileri terimi, bir bireyin AB Temel Haklar Şartı kapsamındaki hak ve özgürlüklerini kullanmasını engelleyebilecek, söz konusu birey ile ilgili en hassas ayrıntılar olarak tanımlanmıştır. Örneğin, bir bireyin etnik kökeni, dini inancı veya cinsel tercihleri ile ilgili bilgiler özel kişisel veri kategorisi sayılır. GDPR, bu durumda söz konusu bilginin ek gizlilik denetimleri kullanılarak korunmasını gerektirir.

Tanım: Bilgi güvenliği

Yeterli bilgi güvenliği olmadan gizliliğin sağlanması mümkün değildir. Bilgi güvenliği PII'nın gizliliğini korumak için gereklidir fakat tek başına yeterli değildir. PII işleme faaliyetlerinin tüm yaşam döngüsü bilgi güvenliği denetimleri yoluyla koruma altına alınmadığı sürece, PII'nın ifşa edilmesini, kaybolmasını veya bozulmasını önlemeye yönelik çalışmalar etkili sonuç veremez. Bilgi güvenliği terimi ISO/IEC 27000:2018 Bölüm 3.28'de, bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini korumaya yönelik yeterli denetimlerin nihai sonucu olarak tanımlanmıştır.

Gizlilik terimi, ISO/IEC 27000:2018 Bölüm 3.10'da bilgilerin söz konusu bilgileri alma yetkisi olmayan kişilere ifşa edilmemesini gerektiren bir bilgi güvenliği özelliği olarak tanımlanmıştır. İfşa; kuruluş dışındaki kişilere kasıtlı olarak bilgi sızdırılması, yanlış kişiye yanlışlıkla bilgi ifşa edilmesi ya da doğru olmayan bir tavsiyeye dayalı olarak bilinçli şekilde yapılan ve dolayısıyla yetkisiz ifşa kapsamına giren bir bilgi aktarımından kaynaklanabilir.

Bütünlük terimi, ISO/IEC 27000:2018 Bölüm 3.36'da bilgilerin doğruluğunun ve eksiksizliğinin korunduğu bir bilgi güvenliği özelliği olarak tanımlanmıştır. Bilgilerin doğruluğu ve eksiksizliği konusunda kullanıcılara güvence vermek için bilgilerin bu özelliklerini güncellemeye yönelik için denetimler mevcut olmalıdır.

Erişilebilirlik terimi, ISO/IEC 27000:2018 Bölüm 3.7'de bilgilerin talep üzerine yetkili kullanıcıların erişimine sunulduğu bir bilgi güvenliği özelliği olarak tanımlanmıştır. Kullanıcıların bilgiye erişim gereklilikleri, iş sürecinin önem düzeyine göre değişiklik gösterecek ve dolayısıyla tüm koşullar altında bilgiyi sağlamak için gerekli düzenlemelerin karmaşıklık düzeyi de değişiklik gösterecektir.

GDPR'nin 5. Maddesinde, kişisel veriler için bir bilgi güvenliği ilkesi tanımlanmıştır. Bu ilke, kişisel verilerin yetkisiz veya yasalara aykırı bir şekilde işlenmesini ve yanlışlıkla kaybolmasını, imha edilmesini veya zarar görmesini önlemeye yönelik uygun teknik veya organizasyonel önlemlerin kullanılmasını gerektirmektedir.

ISO/IEC 29000:2018 Bölüm 3.28'de, bilgi güvenliğinin gerçeklik, sorumluluk, inkar edilemezlik ve güvenilirlik gibi diğer özelliklerinin de bilgi güvenliğinin bir parçası olarak kabul edilebileceği belirtilmektedir. Çoğu uygulayıcı bunları gizlilik, bütünlük ve erişilebilirliğin alt özellikleri olarak görmektedir.

Tanım: Denetim

Denetim, riski gidermeye yönelik bir faaliyettir. ISO/IEC 29000:2018 Bölüm 3.14'te, denetim hedefi terimi, söz konusu denetimin elde etmeyi amaçladığı hedef olarak açıklanmaktadır. Bölüm 3.61'de ise denetim terimi, riski değiştiren ve gizlilik denetimleri bağlamında, gizlilik riskini değiştiren bir önlem olarak tanımlanmıştır. GDPR'de bir denetim veya denetim hedefi tanımlanmamıştır.

İyi uygulamalar belirli gizlilik risklerinin ele alınması için denetim hedeflerinin tanımlanmasını desteklemektedir. Bir gizlilik riski birden fazla gizlilik denetimi hedefi için geçerli olabilir. Her denetim hedefi, organizasyonel ve teknik denetimler dahil olmak üzere, etkili bir operasyonla PII açısından gizlilik riskini ele alabilecek uygun bir dizi denetimin tasarlanmasını gerektirir. ISO/IEC 29000:2018 Bölüm 2.14'te tanımlandığı üzere, gizlilik denetimleri bir gizlilik riskinin gerçekleşme olasılığını azaltır veya sonuçlarını hafifletir. ISO/IEC 27701'e uygunluk için her denetim hedefinin tanımlanması ve denetimlerin bunlardan her birini karşılayacak ve hep birlikte PII'nın gizliliğini destekleyen bir çerçeve meydana getirecek şekilde tasarlanması gerekir.

Tanım: Test

Test bir denetimin tasarımının veya çalışmasının etkililiğini değerlendirme faaliyetidir. Yeterli test yapılmadan, denetimin denetim hedefine ulaşmak için uygun olup olmadığını değerlendirmek imkansızdır. Benzer şekilde, denetimin çalışması yeterli şekilde test edilmeden, denetimin riski gidermedeki etkili olup olmadığını doğru olarak değerlendirmek imkansızdır.

Testle ilgili iyi uygulamalar, önceden bir test planı oluşturulmasını gerektirmektedir. Bu planda aşağıdakiler belirtilmelidir:

- denetim hedefleri
- denetim tasarımının test edilecek özellikleri
- tasarımın değerlendirilmesinde kullanılacak referans kriterler
- denetimin çalışma sırasındaki çıktıları için örnek boyutları
- etkili çalışmayı gösteren eşik kabul düzeyleri
- kabul edilebilir ve kabul edilemez test sonuçları için raporlama sınırları

Gizlilik denetimlerinin testlerinde, PII'yı yöneten iş sürecinin analizinde belirtildiği gibi merkezi kullanım senaryoları göz önünde bulundurulmalıdır. Ancak, hiçbir iş süreci tüm koşullar altında mükemmel çalışmaz. Dolayısıyla, testler için iş süreçlerinin yanlış şekilde çalıştırıldığı veya kötü amaçlı nedenlerle dahili veya harici etkenler yoluyla aksatıldığı kullanım senaryoları da göz önünde bulundurulmalıdır. Yalnızca tüm kullanım senaryoları başarıyla test edildikten sonra gizlilik riskinin kontrol altında olduğu kabul edilebilir.

Harici bilgi kaynakları PII'nın gizliliği açısından risklere katkıda bulunabilir. Örneğin, en aza indirme ilkesi, kuruluşların çok az PII toplamasını gerektirebilir. Bununla birlikte, toplanan PII miktarı ne kadar az olursa olsun, diğer veri kaynaklarıyla birleştirildiğinde, bireylerin tanımlanmasına ve gizliliklerinin risk altına girmesine yol açabilir. Gizlilik riskleri test edilirken, bir bireyi tanımlamak için harici veri kaynaklarının birleştirilerek kullanıldığı senaryolar da göz önünde bulundurulmalıdır. Buna meşhur bir örnek olarak, bir gazetecinin farklı veri kaynaklarını kullanarak bir Bilgi Komiseri adına pasaport başvurusu yaptığı örnek verilebilir.

ISO/IEC 27701'e uygunluk için bir kuruluş, yönettiği PII'nın gizliliğiyle ilişkili risklerin değerlendirildiğini, denetimlerin uygulamaya konulduğunu ve kapsamlı bir denetim testi çerçevesi yoluyla denetimlerin etkin bir şekilde çalıştığını göstermesi gerekir. Dolayısıyla, testler bu sürecin merkezinde yer alır.

Küresel gizlilik düzenlemelerine genel bakış

GDPR'nin uygulanmasında kullanılan temel bilgi kaynağı, Avrupa Veri Koruma Kurulu'dur (EDPB). Kurul, Veri Koruması Etki Değerlendirmeleri yürütülmesi gibi çeşitli konularda çevrimiçi erişime açık kılavuz bilgiler yayınlamaktadır (https://edpb.europa.eu/ guidelines-relevant-controllers-and-processors_en).

EDPB, selefi olan kuruluşun rolünü devralmıştır. Kurulun selefi, 1998 tarihli Veri Koruma Kanunu ile Birleşik Krallık yasalarına dahil edilen 95/46/EC sayılı Veri Koruma Direktifi ile kurulmuş olan "Madde 29 Çalışma Grubu" adıyla anılan bir gruptu. EDPB kurulduğunda 1997'den beri yayınlanan ve çalışanların izlenmesi ve ihlallerin bildirilmesi gibi konuları kapsayan tüm kılavuzları benimsemiştir. Bu kılavuzların tamamı çevrimiçi olarak erişime açıktır (https://ec.europa.eu/justice/article-29/documentation/index_en.htm).

EDPB, kılavuzluğa ihtiyaç duyulduğunu düşündüğü bir alanı incelerken, AB genelindeki Veri Koruma Yetkilileri (DPA'lar) arasında uzlaşma sağlamayı hedeflemektedir. DPA'lar arasında örneğin Birleşik Krallık Bilgi Komisyonu Ofisi (ICO) (www.ico.org.uk) ve Fransa "Commission Nationale de l'Informatique et des Libertes" (CNIL) yer almaktadır.

DPA'lar kişisel verilerin işlenmesini denetleyen kuruluşları tescil etmekten, kuruluş ve bireylere tavsiyelerde bulunmaktan, bireylerden gelen şikayetlere yanıt vermekten ve veri ihlali yaşayan kuruluşları araştırmak ve para cezasına çarptırmaktan sorumludur. DPA aynı zamanda kişisel verileri GDPR'ye uygun olarak işlemediğini düşündüğü kuruluşlara dava açabilir.

GDPR'nin bazı gerekliliklerine uygunluğun nasıl sağlanacağı konusunda hâlâ muğlaklık olsa da, bir DPA'nın uygunsuzluk nedeniyle bir kuruluşa dava açtığı durumlar, DPA'nın ve mahkemelerin kuruluşların yasaya nasıl uymasını beklediğine dair yararlı bir gösterge görevi görecektir. Bir davanın AB temyiz mahkemesi olan Avrupa Adalet Divanı'na temyiz edildiği durumlarda, kararlar nihai karar olarak kabul edilebilir. Bu davalar genellikle bazı karmaşık durumlarda GDPR'nin nasıl uygulanması gerektiğine işaret etmektedir. Bu davaların raporları çevrimiçi olarak yayınlanmaktadır (https://eur-lex.europa.eu/homepage.html?locale=en).

GDPR'nin küresel etkileri

GDPR, verileri nerede işleniyor olursa olsun, Avrupa vatandaşlarının kişisel verilerini kapsamaktadır ve dolayısıyla tüm dünya genelinde kuruluşlar için yüksek bir standart belirlemektedir. Diğer ülkeler, kendi veri koruma yasalarında revizyon yapmayı değerlendirirken, içinde bulunduğumuz küresel sosyal medya çağında veri koruması alanında güncel bir örnek olarak GDPR'yi örnek almıştır. Brezilya, 2020'de yürürlüğe giren ve GDPR'nin birçok ilkesini benimseyen yeni bir veri koruma yasası (LGPD) çıkarmıştır. Ayrıca, yine 2020'de yürürlüğe giren yeni California Tüketici Gizliliği Kanunu (CCPA), GDPR'nin bazı temel kavramlarını benimsemiştir. Washington DC'deki kanun koyucular, CCPA'yı geçersiz kılabilecek bir federal veri gizliliği yasası çıkarmak için müzakerelere devam etmektedir. Bu çalışmalarında GDPR ile benzer düzeyde koruma sağlamaya odaklanmışlardır. Dolayısıyla, GDPR'ye uygunluk, uluslararası yasalara uygunluğu sağlamak için gerekli çaba miktarını azaltmaktadır.

Diğer Avrupa gizlilik yasaları

GDPR şu iki paralel yasa ile aynı zamanda oluşturulmuştur: AB kurumlarında iyi veri koruma uygulamalarının uygulanmasını gerektiren 2018/1725 sayılı Yönetmelik (AB) ve AB kanun uygulayıcı kurumlarında iyi veri koruma uygulamalarının uygulanmasını gerektiren Direktif (680/2016). 2018/1725 sayılı Yönetmelik (AB) 11 Aralık 2018'de yürürlüğe girmiş ve AB kurumları için geçerlidir; Direktif ise her yargı yetki bölgesinde yerel yasalar yoluyla yürürlüğe girmiştir. 2018'de, 23 Mayıs 2018'de yürürlüğe girmiş olan Birleşik Krallık DPA'sına dahil edilmiştir. Çevrimiçi bir kopyasına erişilebilir (http://www.legislation.gov.uk/ukpga/2018/12/ contents).

e-Gizlilik yönetmeliğinden kaynaklanan sorunlar - AdTech iş modeli

AB, 2002 tarihli Gizlilik ve Elektronik Haberleşme Direktifini (2002/58/EC) (e-Gizlilik Direktifi olarak da anılır) güncellemek için GDPR ve Direktife ek olarak yeni bir yasa hazırlamaktadır. Bu Direktif, Birleşik Krallık'ta 2003 tarihli Gizlilik ve Elektronik Haberleşme (EC Direktifi) Yönetmelikleri yoluyla yürürlüğe konulmuş ve "tanımlama bilgisi yasası" olarak anılmaya başlamıştır.

"Tanımlama bilgisi" yasası yürürlüğe girdiğinde web sitelerinin kullanıcıların bilgisayarlarına tanımlama bilgisi yerleştirmek için kullanıcılardan izin istemesini zorunlu kılmıştı. Ancak, yasa bu işlemin nasıl yürütüleceği konusunda çok net bilgiler içermiyordu. Şirketler bir kullanıcının daha önce bilgisayarlarına tanımlama bilgisi yerleştirilmesini reddettiğini belirleyebilmek için bu kullanıcının bilgisayarına, şirketi kullanıcının tercihleri konusunda bilgilendirecek bir tanımlama bilgisi yerleştirmek zorunda kalacakları için endişe duyuyordu. Yasa ayrıca bir kullanıcının bir web sitesini her ziyaret edişinde mi yoksa sadece ilk ziyaret edişinde mi bilgisayarına tanımlama bilgisi yerleştirilmesini kabul etmesi gerekeceği konusunda net değildi. Bu karışıklık nedeniyle, yasa farklı şekillerde yorumlandı ve birçok web sitesi yasanın özüne uymadı.

e-Gizlilik Direktifinde yapılacak revizyonun amacı, 2002'den beri İnternet'te kişisel verilerin işlenmesi alanında meydana gelen değişiklikleri yansıtmak ve GDPR gereklilikleriyle uyumluluğu sağlamaktır. Bu yeni yasa tıpkı GDPR gibi bir yönetmelik şeklinde olacak ve AB genelinde geçerli olacaktır. Yönetmeliğin en son taslak metni (13 Mart 2019), GDPR'de olduğu gibi, elektronik "kişiler arası iletişimin" bir parçası olarak herhangi bir kişisel verinin işlenmesini gizlilik denetimlerine tabi kılmaktadır.

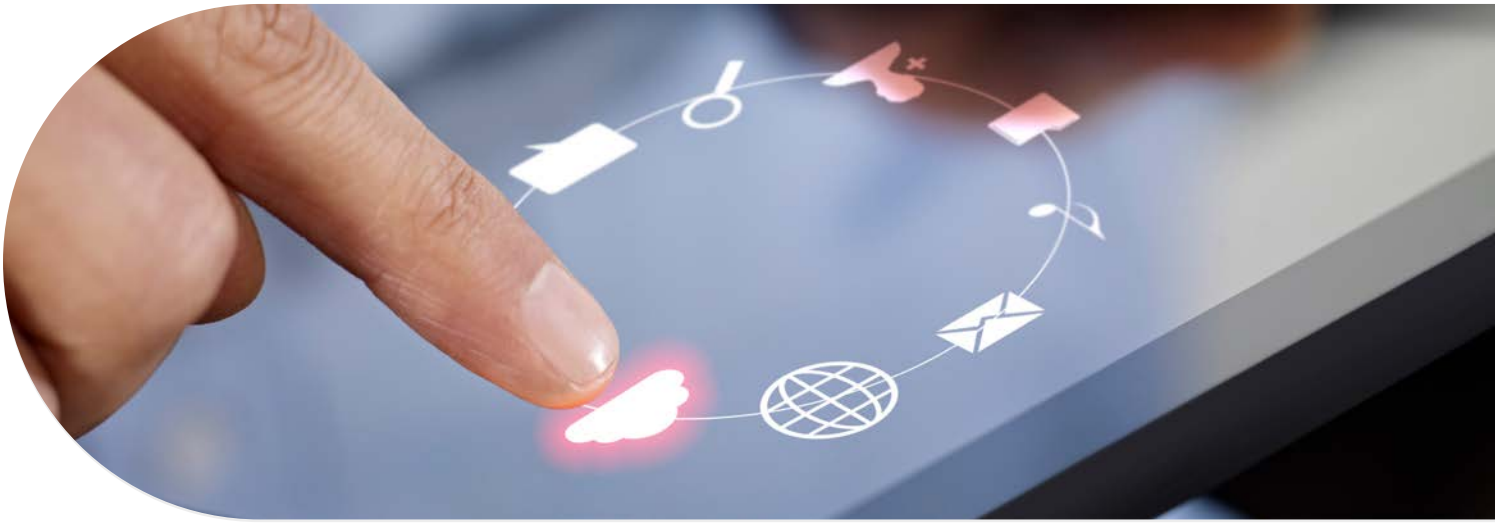
Yönetmeliğin yazımı sırasında meta verilerin işlenmesi de dikkate alınmıştır. Kişisel verilerin çevrimiçi olarak işlenmesiyle ilişkili meta verilerin de kişisel veri olarak sınıflandırılıp sınıflandırılmayacağı henüz karara bağlanmamış olsa da, içtihat hukuku meta verilerin de kişisel veri olarak sınıflandırılması yönünde bastırıyor gibi görünüyor. Bu yönde bir gelişme, meta verilerin de kişisel veriler için kullanılanlara benzer gizlilik denetimleriyle korunmasını gerektirecektir.

Web sitesi ziyaretçilerini ziyaretçinin web sitesindeki etkinliklerini kaydetmeyi amaçlayan tanımlama bilgisi kullanımı konusunda uyarma ihtiyacı, orijinal Direktifin en yaygın olarak bilinen özelliğiydi. Bazı kesimler, ziyaretçileri her ziyaretlerinde uyarma gerekliliğinin yeni Yönetmelikte iptal edilmesini umuyor.

En son taslak metinde, tarayıcı ayarlarında genel bir kabul veya reddetme seçeneğinin kullanılmasına izin verilerek ziyaretçilerin iş yükünün azaltılması amaçlanmaktadır. Ancak, çoğu durumda yine de ziyaretçilerin izin vermesi gerekecek ve izin düzeyinin GDPR'deki izin düzeyini karşılaması, yani iznin "özgür iradeyle verilmiş, spesifik, bilgilendirilmiş ve net" olması beklenmektedir. Web siteleri ayrıca ziyaretçileri kişisel verilerinin nasıl işleneceği ve hangi üçüncü taraflara aktarılacağı konusunda da bilgilendirmek zorunda olacak. Bazı web siteleri tanımlama bilgisi izinleriyle ilgili bilgi bantlarını bu GDPR gerekliliğini yansıtacak şekilde yapılandırmaya başladı bile. Ancak, ICO, web sitelerinin çoğunluğunun henüz GDPR'ye uygun olmadığını belirtmiştir.

Bazı kuruluşlar; işlemeyi kısıtlama, müşterileri bilgilendirme ve izin alma gerekliliğini yerine getirmekte büyük zorluk yaşayacak. Bu zorluğun üstesinden gelemeyen bazı kuruluşlar iş modellerini değiştirmek zorunda kalacaktır. ICO, Haziran 2019'da AdTech'te yayınladığı bir belgeyle kuruluşları bu risk hakkında uyarmıştır (https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf).

e-Gizlilik Yönetmeliğinin 2019'un sonlarında veya 2020'de son haline kavuşması ve 24 ay içinde tüm AB üye devletlerinde otomatik olarak yasalaşması beklenmektedir. Avrupa Ekonomik Alanı'ndaki diğer ülkeler (Norveç, Lihtenştayn ve İsviçre), Yönetmeliğin kendi ülkelerinde yürürlüğe gireceği tarihi müzakereyle belirleyecektir. Belirli ülke kuruluşlarının AB vatandaşlarının kişisel verilerini çevrimiçi olarak işlemek istediği durumlarda, üçüncü ülkelerin e-Gizlilik Yönetmeliğinin gerekliliklerini iki taraflı bir şekilde müzakere etmeleri ve kendi yerel yasalarına yansıtmaları gerekecektir.



Büyük veri sayfalarını işleyenlerin rekabet hukukuyla ilgili karşılaştığı sorunlar

Büyük miktarlarda kişisel veri işleyen kuruluşlar, işleme faaliyetlerinin rekabet hukukunu ihlal edebileceğini keşfediyor.

Rekabet hukuku, hakim bir pazar pozisyonunun aynı pazardaki diğer kuruluşların rekabet etme gücünü azaltacak şekilde kullanılmasını önlemek amacıyla tasarlanmıştır. Sosyal medya platformları gibi kuruluşların yüksek sayıda bireyin kişisel verilerini işlediği durumlarda, bu kuruluşların pazar araştırma verisi toplama ve görüntülü reklam hizmeti sunma konusunda pazarda hakim bir pozisyona sahip olduğu kabul edilebilir. Yeni bir şirket milyonlarca mevcut müşteriye ve onların İnternet verisine sahip olmayacağından, yeni rakip firmalar mevcut bir sosyal medya platformuyla rekabet etmede zorluk yaşayabilir. Bu hakim pozisyonun diğer kuruluşların da pazar araştırma verisi toplamasını engellediği ve pazarda rekabeti azalttığı kabul edilirse, bu sosyal medya platformu rekabet hukuku açısından incelemeye tabi tutulabilir.

AB Komisyonu Rekabet Genel Müdürlüğü, pazarda sağlıklı rekabet açısından bir risk bulunup bulunmadığını tespit etmek için belirli kuruluşların belirli pazarlardaki pazar payına bakmaktadır. Rekabet hukukuna göre pazar araştırma verileri için pazarda hakim pozisyona sahip bir kuruluş tespit ederse, rekabeti engelleyici davranış için para cezaları, iştiraklerin elinden alınması veya hakim grupların bölünmesi gibi yaptırımlar uygulanabilir. Avrupa Komisyonu, yeni düzenlemelerin sosyal medya platformlarının diğer şirketlerden gelebilecek rekabeti azaltmaya yönelik faaliyetlerde bulunmasını nasıl önleyebileceğini aktif bir şekilde değerlendirmektedir.

Çevrimiçi olarak yayınlanan kişisel verilerin doğurabileceği zararlar

Web 2.0 olarak ortamda, kullanıcıların kendi materyallerini çevrimiçi olarak gönderdiği durumlarda, bu materyaller kişisel veri olarak kabul edilebilir. Hosting sitesi bu verilerin gizliliğini korumanın yanı sıra kullanıcı tarafından oluşturulan bu materyallerin üçüncü taraflara zarar verip vermeyeceğini de göz önünde bulundurmalıdır. Birçok ülkede sosyal medya platformlarının, sadece platformun altta yatan teknolojisini sağlayan teknoloji şirketleri olarak düzenlemeye tabi tutulmak yerine bireylerin gönderilerini yayınlayan kuruluşlar olarak düzenlemeye tabi tutulmasını talep eden çağrıların sayısı artış göstermiştir.

Yeni Zelanda'da, 2015 tarihli Zararlı Dijital İletişimler Kanunu, kullanıcı tarafından oluşturulan materyalleri barındıran platformların, spesifik bir içerik hakkında şikayet almaları durumunda, içeriğin yazarı tarafından bu şikayet göz ardı edilse bile söz konusu çevrimiçi materyali silmesini gerektirmektedir. Nisan 2019'da, Birleşik Krallık Hükümeti, kullanıcı tarafından oluşturulan materyalleri barındıran hosting platformlarına "özen borcu" yükümlülüğü getirilmesini öneren bir teknik inceleme yayınlamıştır (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf). Bu öneri yasalaşması halinde, çocuklar veya duyarlı bireyler açısından zararlı materyaller içeren gönderilerin katı bir zaman çerçevesi içinde kaldırılmasını gerektirecektir. İrlanda benzer bir yasa çıkarmayı düşünmektedir. ABD'de sosyal medya platformlarının kullanıcı tarafından oluşturulan materyaller konusunda daha fazla sorumluluk üstlenmesini talep eden çağrılarda bulunulmuştur. ABD Kongresi bu sorunu yeterli düzeyde ciddiye alarak sosyal medya platformlarından çevrimiçi zararlı içerikleri nasıl yönettiklerine dair ifade vermeye çağırmıştır.

Yasada, kullanıcı tarafından oluşturulan materyalleri barındıran platformları, teknoloji şirketleri yerine yayıncı olarak değerlendirme yönünde bir değişim olduğu görülmektedir. Bu durum değişikliği sadece önde gelen sosyal medya platformları için değil, tüm çevrimiçi hosting platformları için önemli sonuçlar doğuracaktır. Kullanıcı tarafından oluşturulan materyal barındıran tüm kuruluşlar, gönderilerin gözden geçirilmesini ve zararlı olduğu kabul edilen gönderilerin derhal silinmesini sağlayacak yeni iş süreçleri geliştirmek zorunda kalabilir.

Gizlilik ve bilgi güvenliği standartlarının uygulanması

Standartlar, gizlilik ve bilgi güvenliği yasa ve düzenlemelerine uygunluğu sağlamak isteyen kuruluşlar için denetim hedefleri açısından bir başlangıç düzeyi sağlanmasına yardımcı olabilir. Birden fazla yasaya uyulması gereken durumlarda, tek bir standart kullanılarak her bir yasal gereklilik kümesi, kuruluşun uygunluk çalışmaları kapsamında üzerinde odaklanabileceği tek bir yapı altında bir araya getirilebilir. Standartları uygulamak bir kuruluşun gizlilik ve bilgi güvenliği denetimlerini uyguladığını ve ayrıca üst yönetimin bu konuları ciddiyetle ele aldığını düzenleyicilere, tedarikçilere ve müşterilere göstermesine imkan sağlar.

GDPR belgelendirmesiyle ilgili sorunlar

EDPB, Haziran 2019'da kuruluşların GDPR'ye uygunluklarını göstermelerine olanak tanıyacak yeni belgelendirme programlarına ilişkin gereklilikler hakkında kılavuz bilgiler yayınlamıştır (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf). Gelecekte büyük olasılıkla GDPR uygunluğuyla ilgili Veri Sahibi Erişim İstekleri, Şikayet Süreçleri, Tasarım Yoluyla Gizlilik ve Veri Sahipleriyle İletişim gibi hususları kapsayan belgelendirme programları geliştirilecektir.

Halihazırda GDPR'yi tüm yönleriyle ele alan bir belgelendirme programı bulunmamaktadır. EDPB yalnızca bazı GDPR denetimlerini kapsayan belgelendirme programlarının, kuruluşların GDPR'ye genel olarak uygunluklarını göstermesine yardımcı olabileceğini belirtmiştir. Bu nedenle, öngörülebilir gelecekte çoğu kuruluşun GDPR belgelendirmesi için birçok farklı belgelendirme programını kullanacağı beklenmektedir.

Gizlilik yönetimi

İyi iş yönetimi, kuruluşların değişen ortam koşullarına yanıt vermesine yardımcı olması açısından önemlidir ve bu konuda destek olabilecek farklı tipte standartlar mevcuttur. Örneğin, yönetim sistemi standartları kuruluşların riski yönetmesine ve kalite yönetimi, sağlık ve güvenlikten gizlilik ve bilgi güvenliğine kadar çok çeşitli alanlarda performansı iyileştirmesine yardımcı olmaktadır.

Yönetim sistemleri yaklaşımının avantajları

Bir iş süreci veya ürün için herhangi bir standarda uymak kuruluşun belirli bir disiplinde gelişmesine yardımcı olur. Ancak bir yönetim sistemleri standardını uygulamak, kuruluş genelindeki tüm fonksiyonları etkileyen çok daha sağlam bir yaklaşım izlenmesini gerektirir. Yönetim sistemleri standardının etkili olabilmesi için kuruluşun mevcut yönetimine dahil edilmesi gerekir.

Yönetim sistemleri standardı, standarda uygunluğu tüm zaman noktalarında sağlam ve uzun vadede ise sürdürülebilir kılmaya odaklıdır. Bu tür bir standart kuruluşa çok daha sistematik ve şeffaf bir yönetim kazandırır. Standarda uygunluk, kuruluşun yönetim sorumluluklarını ciddiye aldığını gösterir.

Liderliğin katılımı

Yönetim sistemleri standardının önemli özelliklerinden biri, kuruluşun üst yönetiminin sürece dahil olmasını gerektirmesidir. Bu, yönetimin gizlilik ve bilgi güvenliği gibi konular üzerinde ciddiyetle durmasını sağlayabilir ve sorunların üst yönetim ekiplerindeki profilinin yükseltilmesine yardımcı olabilir. Ayrıca ileride ek yatırım ve dikkat ihtiyacı hakkında görüşmeler yapılmasına yardımcı olabilir. Çoğu kuruluş için uygunluk yolculuğu hiç bitmeyen bir yolculuktur. Dolayısıyla bir uluslararası standardı uygulamak, ilk enerji patlamasından sonra odağını kaybedebilecek bir program için odak noktasının sürekli korunmasını sağlar.

Entegrasyon verimlilikleri

Bir yönetim sistemleri standardı modüler olarak paylaşılabilecek bir şekilde tasarlanır. Bu yüzden, kuruluşa yeni bir yönetim sistemleri standardı eklemek için gerekli çaba düzeyi en aza iner. Bir kuruluş, örneğin, kalite ile ilgili tek bir yönetim standardını uygulamaya koyduktan sonra ilave bir yönetim standardı (örn. gizlilik ve bilgi güvenliği ile ilgili) eklemek için ilk standarda kıyasla çok daha az çaba gerekir.

Bir yönetim sistemleri standardı yoluyla gizlilik ve bilgi güvenliği gerekliliklerine uygunluğu sağlamayı isteyen her kuruluş böylece, güvenlik veya kalite gibi diğer teknik alanların gelecekte ele alınmasına imkan verecek bir şekilde kendi sağlamlığına ve sürdürülebilirliğine yatırım yapmış olur.

Sonuç

Bu teknik incelemede gizlilik düzenlemeleri ele alınmıştır. Dünya genelindeki gizlilik düzenlemelerinin farklı ve benzer yönleri incelenmiş, e-Gizlilik Direktifi gibi belirli düzenleyici gerekliliklerin önemi vurgulanmıştır.

Tüm düzenlemeler bireylerin gizlilik haklarını savunma şeklinde pozitif bir amaca sahiptir. Bununla birlikte, GDPR'nin hazırladığı zemin, dünya genelindeki diğer ülkeler ve devletler için bir sıçrama tahtası görevi görmektedir. Doğal olarak bunlar arasında kuruluşlar için sorun yaratabilecek nüanslar bulunsa da, uluslararası standartlar bu noktada destek sağlayabilir.

ISO/IEC 27701, kuruluşları kişiyi tanımlamak için kullanılan bilgiler ile ilgili faaliyetlerine yönetimi eklemeye teşvik eden harika bir yönetim sistemleri standardı örneğidir.

Yargı yetki bölgeleri aralarındaki farkların dikkate alınmasını gerektirir ve üst yönetimi gizliliği ciddiyetle ele almaya teşvik eder. Bu, yeni düzenlemelerin çıkarılacağı ve kârlılığı etkileyebileceği durumlarda kritik önem arz eder.

Ayrıca düzenlemelerin karmaşık, sürekli değişen bir yapıya sahip olduğu ve düzenli olarak gözden geçirilmesi gerektiği unutulmamalıdır. Kuruluşlar bir yönetim sistemi yaklaşımını benimseyerek faaliyet gösterdikleri iş ortamı ışığında performanslarını sürekli olarak izlemeye ve değerlendirmeye teşvik edilmektedir. ISO/IEC 27701, kuruluşların, devlet kurumlarının ve akademisyenlerin bilgi birikimlerini bir araya getirerek bu süreci destekleyebilecek bir yönetim çerçevesi oluşturmasına harika bir örnektir.

Yazar

Kieran McDonagh, Riskscape Law Ltd

Kieran McDonagh deneyimli bir veri koruma ve siber güvenlik görevlisidir. Veri koruma, siber güvenlik, iş dayanıklılığı ve tedarik zinciri risk yönetimi alanlarında uygulanan denetimleri denetlemek, risk değerlendirmesine tabi tutmak ve iyileştirmek amacıyla uluslararası standartlardan yararlanmıştır.

BNP Paribas, BP ve Centrica için yasal uygunluk projelerine liderlik eden Kieran McDonagh halihazırda "ISO 31700 - Tasarım Yoluyla Gizlilik" uluslararası standardını geliştiren BSI komitesinin üyesidir. Siber güvenlik, yönetim bilimi ve hukuk alanlarında doktora derecelerine sahiptir.

İnceleyenler

Bu teknik incelemeyi hakem denetiminden geçiren:

Geoffrey Goodell, Kıdemli Araştırma Görevlisi, UCL CBT, UCL Computer Science.
Hakem denetimini yapan bir kişi isminin yayınlanmamasını tercih etmiştir

ISO/IEC 27701 kopyanızı almak için şu bağlantıyı ziyaret edin:
shop.bsigroup.com/bsisoiec27701

Neden BSI?

BSI, 1995'ten beri bilgi güvenliği standartları alanında önde gelen bir kuruluş olarak faaliyet göstermektedir ve bu alanda dünya genelindeki ilk standart olan BS 7799'u geliştirmiş ve güncel olarak dünyanın en popüler bilgi güvenliği standardı olan ISO/IEC 27001'i geliştirmiştir. Üstelik bununla da yetinmeyerek gizlilik, siber güvenlik ve bulut güvenliği gibi alanlarda yeni ortaya çıkan sorunlara yönelik çözümler üretmeye devam ettik. Bu nedenle size yardımcı olmak için en iyi tercih biziz.

193 ülkeden 86.000 müşteriyle çalışan BSI, otomotiv, havacılık ve uzay, yapı sektörü, gıda ve sağlık dahil olmak üzere pek çok sektörde becerileri ve deneyimleriyle gerçekten uluslararası bir kuruluştur. Standart Geliştirme ve Bilgi Çözümleri, Güvence ve Profesyonel Hizmetlerdeki uzmanlığını kullanan BSI, müşterilerinin sürdürülebilir büyüme sağlamasına, riski yönetmesine ve nihayetinde daha dayanıklı olmasına yardımcı olmak için işletme performansını iyileştirir.

Ürünlerimiz ve hizmetlerimiz

Bilgi

Kuruluşumuzun özü, yarattığımız ve müşterilerimize aktardığımız bilgi çevresinde yoğunlaşıyor. Standartlar alanında, uzman bir kuruluş olarak itibarımızı artırmaya devam ediyor ve yerel, bölgesel ve uluslararası düzeylerde standartları şekillendirmek için sektördeki uzmanları bir araya getiriyoruz. BSI, dünyanın en iyi 10 yönetim sistemi standardından sekizini oluşturmuştur.

Güvence

Bir süreç veya ürünün belirli bir standarda uygunluğunun bağımsız şekilde değerlendirilmesi, müşterilerimizin üst düzey bir mükemmellikle performans göstermesini sağlıyor. Standartlardan azami düzeyde faydalanmalarını sağlamak için müşterilerimize birinci sınıf uygulama ve denetleme teknikleri konusunda eğitim veriyoruz.

Uygunluk

Gerçek ve uzun vadeli faydalar sağlamak için müşterilerimizin bir yönetmelik, pazar ihtiyacı veya standarda kesintisiz bir şekilde uyum göstermesi gerekiyor; ancak bu yolla yerleşik bir alışkanlığa dönüşebilir. Bu süreci kolaylaştırmak için çeşitli hizmetler ve farklı yönetim araçları sağlıyoruz.

bsi.

Türkiye Merkez Ofisi
BSI Group Eurasia Belgelendirme Hizmetleri Ltd. Şti.
Değirmen Sokak No. 16
Ar Plaza A Blok Ofis: 61/62
Kozyatağı - İstanbul
Tel. : +90 216 445 90 38 (pbx)
Faks : +90 216 463 26 26
bsi.eurasia@bsigroup.com
www.bsi-turkey.com

BSI ile ISO/IEC 27701 hakkında daha fazla bilgi edinin

Tel: **0216 445 90 38**
web sitesi: **bsigroup.com/tr-TR/**