Getinge Küresel Politikası

Veri Gizliliği Küresel Politikası

Belge sahibi	Anna Romberg
Sürüm	sürüm 3
Yönetim Kurulu tarafından kabul edilir	26 Nisan 2023

1. Özet

Bu Küresel Veri Gizliliği Politikası'nın ("**Küresel Politika**") amacı, temel veri gizliliği gereksinimlerini belirlemek ve Getinge yönetimine, çalışanlarına ve danışmanlarına Kişisel Verilerin İşlenmesini içeren günlük çalışmalarında yönergeler sağlamaktır.

Getinge, Kişisel Verileri yürürlükteki veri koruma yasalarına ve yönetmeliklerine uygun olarak İşlemeyi taahhüt eder. Gizlilik, günlük operasyonlarımızda her zaman birinci öncelik olacaktır.

Bu Küresel Politika, Getinge adına hareket eden tüm çalışanlar, yöneticiler ve iş ortakları için geçerlidir.

2. Tanımlar

Bu Küresel Politikada, aşağıdaki terimler aşağıdaki anlamlara sahiptir:

Veri Sorumlusu	Kişisel Verilerin İşlenmesinin amaçlarını ve vasıtalarını tek başına veya diğer kişilerle birlikte belirleyen tüzel kişilik.
Veri İşleyici	Kişisel Verileri bir Veri Kontrolörü adına İşleyen tüzel kişilik.
Veri Koruma Etki Değerlendirmesi	Bir projeyi, süreci veya çözümü veri koruma üzerindeki etkisi açısından değerlendirmek için sistematik bir süreç.
Veri Koruma Yasaları	GDPR dahil ancak bunlarla sınırlı olmamak üzere yürürlükteki tüm veri koruma yasaları ve düzenlemeleri.
Veri Sahibi	Kişisel Verilerin ilişkili olduğu bireysel kişi.
GDPR	Kişisel verilerin işlenmesi ve bu verilerin serbest dolaşımı ile ilgili olarak gerçek kişilerin korunmasına ve 95/46/EC sayılı Direktifin yürürlükten kaldırılmasına ilişkin 27 Nisan

	2016 tarihli Avrupa Parlamentosu ve Konseyi'nin (AB) 2016/679 sayılı Tüzüğü.
Kişisel veri	Bir Veri Konusu ile ilgili herhangi bir bilgi. Bir Veri Öznesi, bir isim, bir kimlik numarası, konum verileri, çevrimiçi bir tanımlayıcı veya bu gerçek kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü faktörler kullanılarak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir. Kişisel Veriler, iş e-posta adresleri ve irtibat kişileri gibi çalışanların iletişim bilgilerini de içerir.
Kişisel Veri İhlali	İletilen, saklanan veya başka bir şekilde İşlenen Kişisel Verilerin kazara veya yasa dışı olarak imha edilmesine, kaybına, değiştirilmesine, yetkisiz ifşasına veya bunlara erişilmesine yol açan bir güvenlik ihlali.
Kişisel Verilerin İşlenmesi	Toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, geri alma, danışma, iletim yoluyla kullanma, ifşa etme, yayma veya başka bir şekilde kullanıma sunma, hizalama veya birleştirme, kısıtlama, silme veya imha gibi otomatik araçlarla olsun veya olmasın, Kişisel Veriler veya Kişisel Veri kümeleri üzerinde gerçekleştirilen herhangi bir işlem veya işlem kümesi. İşleme, Kişisel Verilerin görüntülenmesini de içerir.
Özel Kişisel Veri Kategorileri-	Yaşayan bir gerçek kişinin ırksal veya etnik kökenini, siyasi görüşlerini, felsefi veya dini inançlarını, cinsel yönelimini, sendika üyeliğini ve faaliyetlerini, genetik veya biyometrik verilerini ve sağlık veya cinsel hayata ilişkin verilerini doğrudan veya dolaylı olarak gösteren tüm Kişisel Veriler.
Denetim Otoritesi	Veri Koruma Yasalarına uyumu izlemekten sorumlu bağımsız bir kamu otoritesi.

3. Kapsam ve amaç

Bu Küresel Politika, tüm Getinge şirketleri, iştirakleri ve ortak operasyonları (müştereken "Getinge") için geçerlidir ve tüm çalışanlarımızın yanı sıra **Getinge** tesislerinde veya Getinge'nin yönetimi altında çalışan danışmanlar ve ajans personeli (hepsi bu Küresel Politikada "**çalışanlar**" olarak anılacaktır) için geçerlidir. Genel kural, bu Küresel Politikanın Getinge içindeki tüm Kişisel Verilerin

İşlenmesi için geçerli olmasıdır. İstisnalar yalnızca bu Küresel Politikada belirtilen durumlarda geçerlidir.

Bu Küresel Politikanın amacı şunları sağlamaktır:

a) Kişisel Veriler ve geçerli Veri Koruma Yasaları hakkında genel bilgi
b) Getinge için birincil öneme sahip yasal gereklilikler hakkında rehberlik
c) Kişisel Verileri İşlerken Getinge için Gereklilikler
d) Getinge Kişisel Verileri İşlerken İzlenmesi Gereken Talimatlar

Bu Küresel Politika ile, Kişisel Verileri Veri Koruma Yasalarına uygun olarak korumayı taahhüt ediyoruz.

4. Uygulama alanı

Uygulanabilirlik hakkında özel

Bu Küresel Politika aşağıdakiler için geçerlidir:

a) Kişisel Verilerin İş Süreçlerinde İşlenmesi
b) Kişisel Verileri İşlemek için kullanılan BT işlevleri, çözümleri veya hizmetleri
c) Outlook, PowerPoint, Word ve Excel gibi araçlar
d) Getinge'nin Kişisel Verilerin üçüncü bir taraf adına İşlenmesini, örneğin hastanelere sağlanan BT çözümlerini içerecek ürün veya hizmetler sağladığı durumlar
e) Getinge'nin bu Küresel Politikada açıklandığı gibi bir Veri Kontrolörü, Veri İşleyici ve/veya Ortak Kontrolör olduğu diğer tüm durumlar

Bu Küresel Politikada belirtilenlerden başka gereklilikler, BT güvenliğiyle ilgili gereklilikler gibi belirli operasyonlar için gerekli olabilir. Bu Küresel Politikaya ek olarak, belirli Getinge ekipleri için geçerli olan Kişisel Verilerin İşlenmesi için ek talimatlar ve yönergeler olabilir.

Geçerli yasalar, yerel gereklilikler ve sapmalar

Bu Küresel Politika, Avrupa veri koruma yasalarına ve düzenlemelerine dayanmaktadır, ancak Getinge'nin AB / AEA dışındaki tüm Kişisel Verileri İşlemesi için de geçerli ve uygulanabilirdir. Avrupa veri koruma yasalarının ve yönetmeliklerinin bu tür İşlemeler için geçerli olmasının nedenleri örneğin şunlar olabilir:

a) İşleme, Getinge'nin AB/AEA'da bulunan genel merkezi tarafından kabul edilen prosedürler, sistemler, rutinler veya kararlarla ilgilidir
b) İşleme, AB/AEA içindeki Veri Sahiplerine sunulan mal ve hizmetlerle veya davranışlarının izlenmesiyle ilgilidir
c) AB/AEA dışındaki kuruluşun, örneğin AB/AEA'da çalışanları olması nedeniyle AB/AEA'da kurulmuş olduğu kabul edilir

Yerel veri koruma yasaları ve yönetmelikleri, bu Küresel Politika tarafından dayatılanlardan farklı veya daha katı gereklilikler getirdiğinde, Getinge bu yasa ve yönetmeliklere uyacaktır. Yasaların ve/veya düzenlemelerin bu Küresel Politika ile çelişmesi durumunda, daha katı olan gereklilik öncelikli olacaktır. Daha fazla rehberlik için lütfen Veri Gizliliği Ekibi ile iletişime geçin.

Anonimleştirilmiş ve takma ad verilmiş veriler

Bu Küresel Politika, *tamamen* anonim olan bilgiler, yani tanımlanabilir bir bireyle ilişkilendirilemeyen bilgiler için geçerli değildir. Günümüz pazarında mevcut olan teknik çözümler nedeniyle, doğru teknik araçları kullanarak bireyleri tanımlamanın birçok farklı yolu vardır. Anonimleştirmenin pratikte elde edilmesinin karmaşık olabileceğini unutmayın.

Bu Küresel Politika, takma ad verme işlemine tabi tutulan bilgiler, yani başka bir bilgi kümesi ("anahtar" gibi) kullanılarak bir bireye bağlanabilen bilgiler için geçerlidir. Takma adlı veriler hala Kişisel Veri olarak kabul edilir.

NOT!

Kişisel Veriler, bir Getinge şirketi tarafından tutulan veriler, başka bir Getinge şirketi veya üçüncü bir tarafça tutulan diğer verilerle birleştirildiğinde anonimleştirilmiş olarak kabul edilmez. Örneğin, statik ve dinamik IP adresleri Kişisel Veri olarak kabul edilir, çünkü IP numarası internet operatörü tarafından tutulan bilgilerle birleştirilirse bireylerle ilişkilendirilebilir. Getinge'nin üçüncü taraflarca tutulan bilgilere erişememesi önemli değildir, yani yine de Kişisel Veri olarak kabul edilir.

5. Uyumluluk sorumluluğu

Veri Gizliliği Ekibi

Getinge'nin Veri Gizliliği Organizasyonu ve Veri Gizliliği Ekibi, Veri Gizliliği Yönetişim Direktifi'nde açıklanmıştır. Veri Gizliliği Ekibi, veri gizliliği alanında gerekli uzman bilgisini koruyacaktır.

Veri Gizliliği Ekibi, Getinge içinde bir tartışma ortağı olarak görülecek ve Veri Gizliliği Ekibinin görüşüne veri gizliliği konularında gereken ağırlık verilecektir.

Daha fazla bilgi için: Veri Gizliliği Yönetişim Direktifi

Getinge şirketlerinin sorumluluğu

Bu Küresel Politikada belirtilen yasalara, yönetmeliklere, dahili Getinge kararlarına, süreçlerine ve prosedürlerine uymak her Getinge şirketinin nihai sorumluluğudur. Ayrıca roller ve sorumluluklarla ilgili Bölüm 19'a bakınız.

Risklerin raporlanması

Getinge, tüm Veri Koruma Yasalarına tam olarak uymaya ve ihlallere yol açan veya potansiyel olarak yol açabilecek iş uygulamalarını proaktif olarak ele almaya ve düzeltmeye çalışacaktır. Her çalışanın, iyi niyetle hareket eden kişiler için misilleme veya diğer olumsuz sonuçlar olmayacağı güvencesiyle, herhangi bir olayı veya uyumsuzluk şüphesini bildirmesi teşvik edilir ve beklenir. Çalışanların, Veri Gizliliği Ekibine veri gizliliği riskleri ve/veya şüpheli uyumsuzluk endişelerini dile getirmeleri beklenir. Endişeler her zaman Bölüm 18'e uygun olarak da dile getirilebilir.

6. Getinge şirketleri Kişisel Verileri Kontrolör veya Ortak Kontrolör Olarak İşlerken Genel Şartlar

Denetleyici

Bir Getinge şirketi Kişisel Verileri İşlediğinde, Kişisel Verilerin neden ve nasıl İşleneceğini belirleyerek bunu kendi inisiyatifiyle yapabilir. Bir Getinge şirketi, Kişisel Verilerin İşlenmesinin araçlarını (nasıl) ve amaçlarını (neden) belirlerse, Veri Kontrolörü olarak adlandırılır.

ÖRNEK

Getinge, her ay maaş ödemek amacıyla çalışanları hakkında Kişisel Veriler toplarsa, Getinge İşlemenin amaçlarını ve araçlarını belirler ve bu nedenle Kişisel Verilerin İşlenmesinin Veri Denetleyicisi olarak kabul edilir.

Ortak Kontrolör

Belirli koşullar altında iki veya daha fazla Veri Kontrolörü, Kişisel Verilerin İşlenmesinin amaçlarını (neden) ve araçlarını (nasıl) birlikte belirleyebilir. Örneğin, bir Getinge şirketi, Veri Denetleyicisi rolünü bir veya daha fazla dahili ve / veya harici kuruluşla paylaşabilir. Buna müşterek kontrolörlük denir.

Ortak bir denetleyici ilişkisi olduğunda, Veri Denetleyicilerinin ilgili sorumluluklarını belirlemek için ortak bir denetleyici sözleşmesi yapmak için yasal bir gereklilik vardır. Getinge şirketi, İntranet'te bulunan ilgili şablonun kullanılmasını sağlayacaktır.

ÖRNEK

Bir Getinge şirketi, Getinge şirketi ve hastanenin işbirliği içinde Kişisel Verilerin proje içinde neden ve nasıl İşleneceğini belirlediği bir hastane ile birlikte bir araştırma çalışması yaparsa, Getinge şirketi ve hastane ortak kontrolör olarak kabul edilebilir ve bu durumda ortak bir kontrolör sözleşmesi yapmak zorunda kalır.

Kişisel Verilerin Toplanması ve İşlenmesi için Temel Şartlar

Kişisel Veriler yalnızca belirli, açık ve meşru amaçlar için İşlenebilir. Amaçların meşru olarak kabul edilebilmesi için, planlanan İşleme, bir Veri Konusunun İşlemeye onay verip vermediğine bakılmaksızın:

a) Meşru bir iş amacına sahip olmak ve herhangi bir Veri Koruma Yasasını veya diğer yasaları ihlal etmemek;
b) Amaçları yerine getirmek için orantılı ve gerekli olmak;
c) Veri Sahipleri üzerinde haksız olumsuz etkileri olan şekillerde kullanılmaması; ve
d) Veri Konularının Kişisel Verilerini yalnızca Veri Konularının makul bir şekilde bekleyeceği şekillerde ele alın.

Kişisel Verilerin Tüm İşlenmesi, İşlemenin amacına ulaşmak için gerekli olmalı ve Veri Sahipleri, Kişisel Verilerinin İşlenmesinin amaçları veya kapsamı konusunda yanıltılmamalı veya aldatılmamalıdır. Kişisel Veriler, Veri Sahibine bildirilen amaçlarla bağdaşmayan hiçbir şekilde İşlenemez. Ayrıca, Getinge şirketleri tarafından İşlenen Kişisel Veriler doğru olmalı ve gerektiğinde güncel tutulmalıdır.

Kişisel Verilerin İşlenmesinin Hukuki Dayanağı

Yasal dayanak hakkında genel

Getinge, Kişisel Verileri yalnızca aşağıdakilerden en az birinin geçerli olması durumunda İşleyebilir:

a) **Kabul.** Veri Sahibi, belirtilen amaç (lar) için İşleme için önceden onay vermiştir. Onay ve onayın geri çekilmesi ile ilgili olarak bu Bölüm 6'da aşağıya bakınız.

b) **Yasal zorunluluk.** Getinge, Getinge'nin tabi olduğu yasal bir yükümlülüğü yerine getirmek için Kişisel Verileri İşlemelidir (vergi geliri bilgilerini vergi makamlarına göndermek gibi).

c) **Bir sözleşmenin ifası.** Kişisel Verilerin İşlenmesi, Getinge'nin Veri Konusu ile yaptığı bir sözleşmedeki yükümlülüklerini yerine getirmesi için gereklidir (bir iş sözleşmesi kapsamında maaşları ödemek için banka hesap bilgilerini saklamak gibi).

d) **Getinge'nin meşru menfaati.** Getinge, Kişisel Verileri işinin bir parçası olarak meşru amaçlar için İşleyebilir (müşterileri veya iş ortakları hakkında bir bilgi veritabanı tutmak veya çalışanları için acil durum irtibat kişilerinin adlarını ve telefon numaralarını toplamak gibi), bu tür çıkarların Veri Konusunun çıkarları veya temel hak ve özgürlükleri tarafından geçersiz kılındığı durumlar hariç. Bu yasal dayanak uygulandığında, söz konusu özel menfaat tanımlanmalı ve Veri Sahibi bu konuda bilgilendirilmelidir.

e) **Başka.** Kişisel Verilerin İşlenebileceği başka nadir gerekçeler de vardır, yani Veri Sahibinin hayati çıkarlarının korunması veya kamu yararına yürütülen görevler.

Onay ve onayın geri çekilmesi

Onay, Getinge şirketleri tarafından yalnızca başka hiçbir yasal dayanak kullanılamadığında kullanılmalıdır. Yasal dayanak olarak onay uygulanırsa, bir Getinge şirketi, Veri Konusunun Kişisel Verilerin İşlenmesine onay verdiğini ve bu onayın geçerli olduğunu gösterebilmelidir. Önceden işaretlenmiş kutular, sessizlik veya hareketsizlik asla onay teşkil etmez. Uygunsa, İşlemenin farklı amaçları için ayrı onaylar alınmalıdır.

Onay:

a) Başka koşullara tabi olmaksızın verilen;
b) Bilgilendirilmiş (Veri Sahiplerine yönelik bilgiler hakkında bu Bölümde aşağıya bakınız);
c) Gönüllü olarak sağlanmıştır (Veri Konusu onay vermek için baskı altında hissetmemelidir); ve
d) Belirli ve açık (Veri Sahibi, onayın kapsamının farkında olmalıdır).

Onay yazılı olarak veya elektronik olarak verilmelidir. Bir Veri Öznesinin önerilen Kişisel Verilerin İşlenmesini kabul edip etmediği açıkça belirtilmelidir. Sessizlik veya hareketsizlik nedeniyle onay verilemez.

Veri Sahibi, verilen onayı istediği zaman geri çekebilir. Onay geri çekildiğinde, ilgili Getinge şirketi, İşlemenin izne dayandığı ölçüde, Veri Konusu hakkındaki Kişisel Verilerin İşlenmesini durduracaktır. Bu, onayı geri çeken kişi hakkındaki tüm Kişisel Verilerin, yedeklemelerdeki Kişisel Veriler de dahil olmak üzere silinmesi veya anonimleştirilmesi gerektiği anlamına gelir.

Özel Kişisel Veri Kategorilerinin İşlenmesi için Ek Gereklilikler

Genellikle "Hassas Kişisel Veriler" olarak adlandırılan Özel Kişisel Veri Kategorileri, özel koruma altındadır ve özel durumlar dışında Getinge tarafından İşlenmemelidir.

Özel Kişisel Veri Kategorilerinin İşlenmesi, yalnızca yukarıda bu Bölüm 6'da açıklandığı gibi İşleme için yasal bir dayanak varsa gerçekleştirilebilir. Buna ek olarak, bu tür veriler yalnızca aşağıdaki koşullardan en az birinin yerine getirilmesi durumunda İşlenebilir:

a) Veri Sahibi, belirtilen amaç(lar)lar için İşlemeye açık rıza vermiştir;
b) İşlemenin, ulusal kanunlar veya toplu sözleşmeler tarafından izin verildiği ölçüde, Veri Kontrolörünün veya Veri Sahibinin iş hukuku alanındaki yükümlülüklerini yerine getirmesi ve haklarını kullanması amacıyla gerekli olması;
c) İşlemenin yasal bir iddianın oluşturulması, uygulanması veya savunulması için gerekli olması; veya
d) İşleme, koruyucu veya mesleki tıp amacıyla, çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi teşhis, sağlık hizmeti veya tedavinin sağlanması için gereklidir.

Getinge genellikle Özel Kişisel Veri Kategorilerini İşlemekten kaçınmalıdır ve bunu yalnızca yukarıdakilerden biri veya daha fazlası geçerliyse yapabilir. Yerel istisnalar da geçerli olabilir.

NOT!

Açık rıza, rıza ve rızanın geri çekilmesi ile ilgili olarak yukarıda Bölüm 6'da açıklandığı gibi düzenli bir rızanın gerekliliklerini içerir. Buna ek olarak, bireye önerilen Kişisel Verilerin İşlenmesine katılma veya katılmama seçeneği açıkça sunulacaktır.

Cezai suçlar ve mahkumiyetler kapsamında Kişisel Veriler

Getinge, yürürlükteki yasa ve yönetmeliklerin izin verdiği veya gerektirdiği durumlar dışında, şüpheler de dahil olmak üzere cezai suçlar veya mahkumiyetlerle ilgili hiçbir Kişisel Veriyi İşleymeyecektir. Bu tür Kişisel Verilerin İşlenmesi için genel bir yasak olduğunu unutmayın. Bununla birlikte, ulusal yasa ve yönetmeliklerde muafiyetler bulunabilir.

Cezai suçlar, mahkumiyetler veya ilgili şüphelerle ilgili Kişisel Verileri İşlemek için farklı Getinge departmanlarında gereksinimler olabilir. Örneğin, soruşturmalar ve/veya durum tespiti bağlamında, Hukuk, Uyum ve Yönetişim departmanında ilgili pozisyonlardaki şirketler ve/veya personel üzerinde olgu bulma, geçmiş kontrolleri gerçekleştirme gereklilikleri (yürürlükteki yasa ve yönetmeliklerle desteklendiği durumlarda) vardır.

NOT!

Sabıka kayıtları, cezai suçlar, mahkumiyetler veya ilgili şüphelerle ilgili herhangi bir Kişisel Verinin İşlenmesinden önce Veri Gizliliği Ekibine her zaman danışılacaktır.

Veri Sahiplerine Bilgi

Getinge, Veri Sahiplerine aşağıdaki konularda bilgi içeren yazılı bildirimde bulunacaktır:

a) Veri Sorumlusu olan işletmenin adı ve iletişim bilgileri;
b) İşlenen Kişisel Verilerin türleri ve İşlemenin ilgili amaçları;
c) İşlemenin yasal dayanağı;
d) Kişisel Verilerin ne kadar süreyle saklanacağı;
e) Kişisel Verilerin alıcıları veya alıcı kategorileri;
f) Aşağıdaki Bölüme 8 uygun olarak Veri Sahibinin hakları hakkında bilgi; ve
g) Varsa:
    i. sorumlu Veri Koruma Görevlisinin iletişim bilgileri;
    ii. Kişisel Verilerin elde edildiği yer;

iii. Bir Veri Öznesinin Kişisel Verilerini sağlamamasının sonuçları;
iv. Getinge'nin Kişisel Verileri aşağıdaki Bölüme 9 uygun olarak AB / AEA dışına aktarma niyetleri; ve
v. Profil oluşturma hakkında bilgi.

Veri Gizliliği Ekibi, bir Getinge şirketinin Veri Konularını Kişisel Verilerin İşlenmesi hakkında bilgilendirmesi gerektiğinde her zaman kullanılacak şablon gizlilik bildirimleri sağlar. Şablonlar, Veri Sahiplerine sağlanması gereken bilgiler hakkında daha fazla talimat içerir.

Gizlilik bildirimlerinin yeterli ve eksiksiz olduğundan ve Veri Koruma Yasalarına uyduğundan emin olmak ve göstermek her Getinge şirketinin sorumluluğundadır. Buna ek olarak, Getinge şirketleri gerekirse gizlilik bildirimlerini yerel dile çevirecektir.

Çalışanlarla ilgili olarak, Kişisel Verilerin İşlenmesi ile ilgili bilgiler genellikle çalışanların iş sözleşmesiyle birlikte aldıkları Çalışan Gizlilik Bildiriminde sağlanır. Her Getinge şirketi, Çalışan Gizlilik Bildiriminin çalışanlar tarafından kolayca erişilebilir ve güncel olmasını sağlamanın yanı sıra, şirketin çalışanlarla ilgili Kişisel Verileri nasıl İşlediği hakkında yeterli bilgi sağlayacaktır.

Kişisel Verilerin İşlenme Amaçlarının Değiştirilmesi

Kişisel Verilerin İşlenme amaçlarını değiştirmeden önce, bir Getinge şirketi şunları yapacaktır:

a) Kişisel Verilerin İşlenmesinin yasallığını değerlendirmek ve değerlendirmeyi aşağıdaki Bölüm 7'ye uygun olarak belgelemek;
b) Veri Sahibine, İşlemenin amaçlarındaki değişiklikleri açıklayan yazılı bilgi sağlamak; ve
c) İşleme izne dayanıyorsa, Veri Sahibinden yeni bir onay alın.

Profil oluşturma ve otomatik karar verme

Profil oluşturma hakkında genel bilgiler

Profil oluşturma, bir Veri Konusu ile ilgili kişisel yönleri değerlendirmek veya Veri Sahibinin işteki performansını, ekonomik durumunu, konumunu, sağlığını, kişisel tercihlerini, ilgi alanlarını, güvenilirliğini veya davranışını, sürücü davranışını, müşteri davranışını, konumunu veya hareketini tahmin etmek veya analiz etmek amacıyla Kişisel Verilerin otomatik olarak işlenmesini gerektirir.

Profil oluşturma genellikle çeşitli kaynaklardan gelen verileri kullanarak bireyler hakkında tahminlerde bulunmak ve istatistiksel çıkarımlar yapmak için kullanılır. İşlemenin amacı, Veri Sahibinin özelliklerini veya davranış kalıplarını belirli bir gruba veya kategoriye yerleştirmek için analiz etmek olabilir. Bu, Veri Kontrolörünün, örneğin Veri Sahibinin çıkarları, bir görevi yerine getirme yeteneği veya olası davranışları hakkında tahminlerde bulunmasını sağlar.

ÖRNEKLER

Profil oluşturma, örneğin, belirli ürünler veya hizmetlerle ilgili kişiselleştirilmiş reklamlar göndermek için bir bireyin web sitelerindeki davranışını çerez tanımlayıcıları veya IP adresleri aracılığıyla analiz etmekten oluşabilir. Profil oluşturmanın bir başka örneği, gelecekteki satın alımları tahmin etmek için önceki satın alımların analizi ile ilgilidir. Bu nedenle, profilleme,

doğrudan pazarlama ve sosyal medya ile bağlantılı olarak yaygın olarak kullanılan bir yöntemdir, ancak araştırma çalışmalarında olduğu gibi diğer İşleme faaliyetleri için de kullanılabilir.

Profil oluşturmaya dayalı kararlar

Bir Getinge şirketi tarafından profillemeye dayalı olarak verilen bir karara yalnızca aşağıdaki durumlarda izin verilecektir:

a) Veri Sahibi ile Veri Kontrolörü arasında bir anlaşmanın yapılması veya yerine getirilmesi için kesinlikle gerekli olması (bu istisna dar yorumlanmalıdır);
b) kurumların veya ulusal gözetim organlarının düzenlemelerine, standartlarına ve tavsiyelerine uygun olarak yürütülen dolandırıcılık ve vergi kaçakçılığı izleme ve önleme amaçları da dahil olmak üzere yasalarca açıkça yetkilendirilmiştir; veya
c) Veri Sahibi açık rıza vermiştir.

Gereksinim -leri

Getinge şirketleri, profil oluşturma yaparken aşağıdakileri sağlamalıdır:

a) Sadece amacı yerine getirmek için gerekli Kişisel Verileri İşlemek;
b) Veri Sahiplerine, Bölüm 6'ya uygun olarak profil oluşturma hakkında yeterli bilgi sağlayın. Profil oluşturma otomatik karar verme ile ilgiliyse, Veri Konularının ulaşılan karar hakkında bir açıklama ve bu karara itiraz etme hakkı hakkında bilgi edinme hakkı vardır;
c) Profil oluşturma için yeterli matematiksel veya istatistiksel prosedürleri kullanın;
d) Bölüme 0uygun olarak uygun teknik ve organizasyonel önlemleri uygulamak; ve
e) Kişisel Verileri, Veri Sahiplerinin hak ve çıkarları için söz konusu olan potansiyel riskleri dikkate alan ve diğerlerinin yanı sıra, Özel Kişisel Veri Kategorileri temelinde bireylere karşı ayrımcı etkileri önleyen veya bu etkiye sahip önlemlerle sonuçlanan bir şekilde güvence altına almak.

NOT!

Profil oluşturma, gerçekleştirilmeden önce Veri Gizliliği Ekibi tarafından önceden onaylanacaktır.

Kişisel Verilerin saklanması, saklanması ve silinmesi

Getinge şirketleri, Kişisel Verilerin aşağıdakilerden daha uzun süre İşlenmemesini sağlayacaktır:

a) İşlemenin amaç(lar)ı ile ilgili olarak gerekli; ve
b) Veri Koruma Yasaları tarafından izin verilir.

Getinge şirketleri, bu Bölümdeki gerekliliklerin yerine getirilmesini sağlamak için işlenmiş olarak uygulanacaktır.

NOT!

Bazı ülkeler (örneğin Rusya ve Çin), vatandaşlarıyla ilgili tüm Kişisel Verilerin ilçe sınırları içinde saklanmasını gerektirir. Diğer ülkelerde, belirli amaçlar için İşlenmişse belirli Kişisel Verilerin yerel olarak saklanması gerekebilir (örneğin, İsveç, muhasebe bilgilerinin kendi sınırları içinde saklanmasını gerektirir). Yerelleştirme gereksinimleri normalde Getinge'nin Kişisel Verilerin bir kopyasını başka bir yerde saklamasını engellemez, eğer böyle bir depolama gerekliyse.

7. İşlemenin değerlendirilmesi ve belgelendirilmesi

İşleme faaliyetlerinin kaydı

Veri Koruma Yasaları gerektirdiğinde, Getinge şirketleri, şirketlerin İşleme faaliyetlerinin kaydını tutmaktan sorumludur. Tüm kayıtlar, Veri Gizliliği Ekibi tarafından seçilen ve işlenen uyumluluk aracında tutulacaktır. Daha fazla bilgiyi Veri Gizliliği İntranet sayfasında bulabilirsiniz.

Bu Bölümdeki gereklilikler hem Getinge şirketleri Veri Kontrolörleri hem de Veri İşleyicileri olarak hareket ederken geçerlidir.

Yeni bir İşleme faaliyeti başlatmadan önce yasallığın değerlendirilmesi

Yeni bir İşleme faaliyeti yürütmeden veya devam eden bir faaliyette değişiklik yapmadan önce, Getinge şirketleri Kişisel Verilerin İşlenmesinin yasallığını değerlendirecek ve değerlendirmeyi belgeleyecektir. Bu, daha önce değerlendirilmemiş ve/veya belgelenmemiş devam eden İşleme faaliyetleri için de geçerlidir.

Bu Bölümdeki gereklilikler hem Getinge şirketleri Veri Kontrolörleri hem de Veri İşleyicileri olarak hareket ederken geçerlidir.

Veri Koruma Etki Değerlendirmeleri

Kişisel Verilerin İşlenmesinin, Veri Sahiplerinin hak ve özgürlükleri için yüksek bir riskle sonuçlanması muhtemel ise, Getinge şirketleri, öngörülen bu İşleme başlatılmadan önce, İşleme operasyonlarının Kişisel Verilerin korunması üzerindeki etkisinin bir değerlendirmesini yapacaktır (Veri Koruma Etki Değerlendirmesi). Bir Veri Koruma Etki Değerlendirmesi, Getinge şirketleri yeni teknolojiler kullandığında ve İşlemenin doğasını, kapsamını, bağlamını ve amaçlarını dikkate aldığında özellikle ilgili olabilir.

Veri Koruma Etki Değerlendirmeleri her zaman bir Getinge şirketi adına Veri Gizliliği Ekibi tarafından gerçekleştirilecektir. Getinge şirketi, gerekli bilgilerin sağlanması da dahil ancak bunlarla sınırlı olmamak üzere, değerlendirme sırasında Veri Gizliliği Ekibi ile işbirliği yapacaktır.

8. Veri Sahibi hakları

Veri Sahibi taleplerinin ele alınması

Veri Sahiplerinden gelen taleplerle ilgili olarak aşağıdakiler geçerlidir:

a) Veri Sahiplerinden gelen tüm talepler derhal Veri Gizliliği Ekibine iletilecek ve Veri Gizliliği Ekibi tarafından ele alınacaktır.
b) Veri Sahipleri, Veri Sahipleri haklarını kullanırken olumsuz sonuçlarla karşılaşamazlar.
c) Tüm Veri Sahibi talepleri gizlilik içinde ele alınacaktır.
d) Getinge şirketleri, Veri Gizliliği Ekibinin taleplere zamanında cevap verebilmesi için Veri Gizliliği Ekibi ile işbirliği yapacaktır.

Veri Sahibi haklarının mutlak olmadığını ve istisnaların geçerli olabileceğini unutmayın.

Veri Sahibi haklarını işleme süreçleri

Getinge şirketleri, Veri Gizliliği Ekibine Veri Konularının aşağıdaki haklarının ele alınmasında yardımcı olacak süreçlerin uygulanmasından sorumludur:

a) Kişisel Verilere erişim talep etme. Buna, Veri Konularının, söz konusu bireyle ilgili Kişisel Verilerin İşlenmesi hakkında bilgi alma ve veri taşınabilirliği hakkını sağlama hakkı da dahildir.
b) Yanlış Kişisel Verilerin düzeltilmesini talep etme.
c) Kişisel Verilerin silinmesini talep etme.
d) İşlemenin Getinge'nin meşru menfaatine dayandığı durumlarda, İşlemenin profil oluşturma ile ilgili olduğu durumlar da dahil olmak üzere, Kişisel Verilerin İşlenmesine herhangi bir zamanda itiraz etmek.
e) Kişisel Verilerin kısıtlanmasını sağlamak.

9. Kişisel Verilerin Aktarılması

Transferler hakkında genel

Kişisel Veriler yalnızca İşlemenin amaç(lar)ını yerine getirmek için aktarılacaktır. Kişisel Verilerin aktarılması, Kişisel Verilerin yalnızca e-posta gibi elektronik iletilerin kullanılmasıyla gönderilmesini değil, aynı zamanda Kişisel Verilere ne zaman erişilebileceğini veya görüntülenebileceğini de içerir. Kişisel Veriler, yalnızca geçici olarak erişilse, görüntülense veya başka bir şekilde İşlenmiş olsa bile aktarılmış olarak kabul edilir.

ÖRNEK

Kişisel Veriler, Fransa'daki bir Getinge şirketi Kişisel Verileri Çin'deki Getinge çalışanları tarafından erişilebilen bir klasörde sakladığında aktarılır (ayrıca Kişisel Verilerin AB/AEA'dan AB/AEA dışındaki bir ülkeye aktarılmasıyla ilgili olarak bu Bölüm 9'a bakınız).

Kişisel Verilerin AB/AEA'dan AB/E EAdışındaki bir ülkeye aktarılması

Ana kural olarak, AB/AEA'daki Getinge şirketleri, Kişisel Verileri AB/AEA dışına aktarmayacaktır. Bu tür transferler yalnızca kesinlikle gerekli olduğunda yapılabilir.

Kişisel Verilerin AB/AEA'daki ülkelerden AB/AEA dışındaki ülkelere aktarılması kesinlikle gerekliyse, Getinge şirketleri şunları sağlayacaktır:

a) Bu tür aktarımlar, aşağıdakilere dayalı aktarımlar dahil ancak bunlarla sınırlı olmamak üzere, Veri Koruma Yasalarına uygun olarak yeterli önlemlere tabidir:
    i. Avrupa Komisyonu tarafından verilen bir yeterlilik kararı;
    ii. Avrupa Komisyonu tarafından kabul edilen AB Standart Sözleşme Maddeleri; veya
    iii. Açık rıza.
b) Gerekirse Transfer Etki Değerlendirmesi yapılmıştır.

Kişisel Verilerin aktarılmasından önce, Veri Konuları, Bölüm 6'ya uygun olarak aktarım ve uygulanabilir yeterli koruma hakkında bilgi alma hakkına sahiptir.

10. Getinge içinde Kişisel Verilerin Paylaşılması ve İfşası

Getinge çalışanları ve danışmanları, Kişisel Verileri yalnızca Getinge içinde iş görevlerinin yerine getirilmesi için bu tür verilere ihtiyaç duyan ve bu Kişisel Verilerin paylaşılması veya ifşa edilmesi için meşru bir iş amacı olan bireylerle paylaşacak ve ifşa edecektir. Kişisel Veriler, yalnızca İşlemenin amaç(lar)ını yerine getirmek için gerekli olduğu ölçüde paylaşılabilir veya açıklanabilir. Kişisel Veriler paylaşılamaz veya açıklanamaz, çünkü alıcı için "sahip olmak güzel" olabilir.

11. Veri İşleyiciler

Sözleşmelerdeki maddeler hakkında genel

Gerekirse, Getinge'nin standart iş ve istihdam sözleşmelerine Kişisel Veri İşleme maddelerini ve / veya veri işleme sözleşmelerini dahil etmek Getinge şirketlerinin sorumluluğundadır.

Mevcut anlaşmaların halihazırda yürürlükte olduğu durumlarda, Getinge şirketleri bu tür sözleşmeleri gerektiğinde Kişisel Veri İşleme maddeleri ve / veya ilgili veri işleme sözleşmeleri ile güncelleyecektir.

NOT!

Veri Gizliliği İntranet sayfasında bulunan veri işleme sözleşmesi şablonları her zaman bir veri işleme sözleşmesinin gerekli olduğu durumlarda kullanılmalıdır.

Üçüncü taraflarla ilgili olarak Veri İşleyici olarak Getinge

Bir Getinge şirketi Kişisel Verileri üçüncü bir taraf (müşteri gibi) adına İşliyorsa, Getinge ve üçüncü taraf bir veri işleme sözleşmesi imzalayacaktır. Getinge şirketi, İntranet'te bulunan ilgili şablonun kullanılmasını sağlayacaktır.

ÖRNEK

Getinge, çoğu durumda, yazılım çözümlerimizin hastanelere sağlanmasıyla bağlantılı olarak Veri İşleyici olarak hareket etmektedir. Bu, Getinge'nin yazılım desteği sağladığımızda Kişisel Verilere erişmesi veya başka bir şekilde İşlemesi gerektiğinde geçerlidir. Bu durumlar için hastane Veri Sorumlusu sıfatıyla hareket edecektir.

Harici Veri İşleyici ile Sözleşme Yapma

Üçüncü bir taraf Getinge adına (tedarikçi gibi) Kişisel Verileri İşleyecekse, Getinge ve üçüncü taraf bir veri işleme sözleşmesi imzalayacaktır. Getinge şirketi, İntranet'te bulunan ilgili şablonun kullanılmasını sağlayacaktır.

ÖRNEK

Getinge, BT sisteminin/çözümünün tedarikçisinin Getinge adına Kişisel Verileri İşlemesini (Kişisel Verileri depolamak ve / veya destek sağlarken Kişisel Verilere erişmek gibi) içeren yeni

bir BT sistemi / çözümü satın alırsa, Getinge ve tedarikçi bir veri işleme sözleşmesi imzalayacaktır. Bu durumda, Getinge Veri Kontrolörüdür ve tedarikçi Veri İşleyicidir.

Diğer Getinge şirketleriyle ilgili olarak Veri İşleyici olarak Getinge

Bir Getinge şirketi Kişisel Verileri başka bir Getinge şirketi adına İşliyorsa, taraflar grup içi bir veri işleme sözleşmesi imzalayacaktır. Getinge şirketleri/fonksiyonları şunları sağlayacaktır:

a) Veri Gizliliği İntranet sayfasında bulunan ilgili şablon kullanılır; veya
b) Grup içi bir veri işleme sözleşmesi zaten imzalanmıştır.

ÖRNEK

Getinge IT, Getinge HR'ye Getinge HR adına Kişisel Verileri İşlemesini içeren destekle yardımcı olursa, grup içi bir veri işleme sözleşmesi imzalanacaktır. Bu durumda, Getinge IT Veri İşleyici ve Getinge HR Veri Denetleyicisidir.

12. Teknik ve organizasyonel güvenlik önlemleri

Tüm Getinge şirketleri, Getinge'nin bilgi güvenliği ile ilgili politika ve direktiflerine uyacaktır. Getinge şirketleri ayrıca riske uygun bir güvenlik seviyesi sağlamak için uygun teknik ve organizasyonel önlemleri uygulamalıdır. Bu tür önlemler uygulanırken aşağıdakiler dikkate alınmalıdır:

a) Son teknoloji;
b) Uygulama maliyeti;
c) İşlemenin niteliği, kapsamı ve amaçları; ve
d) Veri Sahiplerinin hak ve özgürlükleri için olasılık ve önem derecesi riski.

Kişisel Verilerin İşlenmesinin, erişim hakları, Kişisel Verilerin silinmek üzere işaretlenmesi, otomatik silme ve verilerin günlüğe kaydedilmesi gibi uygun teknik ve organizasyonel önlemlerin alınması da dahil olmak üzere Veri Koruma Yasalarına uygun olmasını sağlamak her Getinge şirketinin sorumluluğundadır. Erişim haklarıyla ilgili olarak, Getinge şirketleri, Kişisel Verilere erişimin, Getinge içindeki rollerin değişmesi de dahil olmak üzere, çalışanların ve danışmanların rollerini yansıtmasını sağlayacaktır.

13. BT çözümleri Kişisel Verilerin İşlenmesi

Kişisel Verileri İşlemek için kullanılan yeni ve mevcut BT işlevlerinin, çözümlerinin ve / veya hizmetlerinin, aşağıdakilerle ilgili gereklilikler dahil ancak bunlarla sınırlı olmamak üzere, Veri Koruma Yasalarına uygun olmasını sağlamak her Getinge şirketinin sorumluluğundadır:

a) Tasarım gereği ve varsayılan olarak gizlilik;
b) Veri saklama;
c) Veri taşınabilirliği dahil olmak üzere Veri Sahibi talepleri;
d) Yeterli teknik ve organizasyonel güvenlik önlemleri; ve
e) Erişim hakları.

Yeni bir BT çözümü kullanılmadan ve mevcut bir BT çözümünde değişiklikler yapılmadan önce, Getinge şirketleri Veri Gizliliği Ekibini gizlilik riskleri, amaçları ve İşlenen Kişisel Veriler hakkında zamanında bilgilendirecektir. Mevcut BT çözümlerinde Kişisel Verilerin İşlenmesi hakkında Veri Gizliliği Ekibine de bilgi verilecektir.

Daha fazla bakınız: Bilgi Güvenliği Direktifi

14. Tasarım gereği ve varsayılan olarak gizlilik

Getinge, Kişisel Pata'nın İşlenmesini içeren uygulamaları, hizmetleri ve ürünleri geliştirirken, tasarlarken, seçerken ve kullanırken tasarım gereği ve varsayılan olarak gizlilik ilkeleri dikkate alınmalıdır. Bu ilkeler hem İşleme araçlarının belirlenmesi sırasında hem de İşlemenin kendisi sırasında uygulanmalıdır.

Tasarım gereği gizlilik, mühendislik süreci boyunca veri korumasını dikkate alan bir sistem mühendisliği kavramı ve yaklaşımıdır. Tasarım gereği gizlilik, gizliliğin en başından itibaren bilgi teknolojisine, iş süreçlerine, fiziksel alanlara ve ağa bağlı altyapılara gömülmesini sağlamaya odaklanır.

Getinge, sistemlerinin ve süreçlerinin özellikle veri koruması göz önünde bulundurularak tasarlandığından emin olmalıdır. Veri koruması sonradan düşünülmüş bir düşünce olmamalı, işletmenin işini nasıl yürüttüğünün dokusuna dahil edilmelidir.

Varsayılan olarak gizlilik, Veri Kontrolörünün, varsayılan olarak, İşlemenin her bir özel amacı için yalnızca gerekli Kişisel Verilerin İşlenmesini ve özellikle hem veri miktarı hem de depolama süresi açısından bu amaçlar için gerekli olanın ötesinde toplanmamasını veya saklanmamasını sağlamak için mekanizmalar uygulayacağı anlamına gelir. Özellikle, uygulanan mekanizmalar, Kişisel Verilerin varsayılan olarak belirsiz sayıda birey tarafından erişilebilir kılınmamasını sağlayacaktır.

ÖRNEK

Örnek olarak, Getinge Kişisel Verileri depolamak veya bunlara erişmek için yeni BT sistemleri oluştururken, veri gizliliği etkileri olan politikalar veya stratejiler geliştirirken, Kişisel Veri paylaşımını veya kullanımını yeni amaçlar için başlattığında gizliliği tasarım gereği ve varsayılan olarak dikkate almak uygun olacaktır.

Projeleri, süreçleri, ürünleri veya sistemleri tasarım gereği ve başlangıçta varsayılan olarak göz önünde bulundurarak gizlilik içinde tasarlamanın aşağıdakiler de dahil olmak üzere çeşitli avantajları vardır:

a) Potansiyel sorunları, genellikle ele almanın daha basit ve daha az maliyetli olduğu erken bir aşamada belirleme olasılığı;
b) Kurum genelinde veri gizliliği bilinci artırılır;
c) Veri Koruma Yasalarının yükümlülüklerini yerine getirme olasılığı artar ve eşit olarak ihlal olasılığı azalır; ve
d) Projelerin, süreçlerin, ürünlerin veya sistemlerin gizliliğe müdahaleci olma ve bireyler üzerinde olumsuz bir etkiye sahip olma olasılığı daha düşüktür.

Özellikle Getinge, Kişisel Verilerle ilgili ürün ve hizmetler tasarlarken ve geliştirirken, Getinge'nin tasarım ve varsayılan gereklilikler gereği gizliliğe nasıl uyması gerektiğine dair ilgili detaylar tanımlanmalıdır.

15. Kişisel Veri İhlalleri

Tüm Kişisel Veri İhlalleri, Veri Gizliliği İntranet sayfasında açıklanan sürece uygun olarak derhal bildirilecektir.

Getinge şirketleri:

a) Kişisel Verilerin İşlenmesi için kullanılan tüm çözümlerin Kişisel Veri İhlallerinin raporlanmasını sağlamasını sağlamak;
b) Kişisel Veri İhlallerinin tespitini destekleyen tedbirleri uygulamak;
c) etkileri, olası riskleri ve alınan veya planlanan çözümler dahil olmak üzere Kişisel Veri İhlalinin koşullarını belgelemek; ve
d) Kişisel Veri İhlalleri soruşturulduğunda ve giderildiğinde Veri Gizliliği Ekibi ile işbirliği yapmak.

Daha fazla bakınız: Kişisel Veri İhlali Direktifi

16. Denetim Makamları

Denetim Otoriteleri ile tüm temaslar Veri Gizliliği Ekibi tarafından ele alınacaktır. Getinge şirketleri, talep üzerine Denetim Makamları ile işbirliği yapacaktır.

17. Sapmalar

Bu Küresel Politikadan sapmalar, Küresel Politikanın ilk onaylandığı tarihle aynı yetki düzeyinde onaylanacaktır.

18. Küresel Politikaya Karşı İhlaller – Sesini Yükselt

Bir endişenizi dile getirmekten çekinmeyin. Bu Küresel Politikanın ihlal edildiğinden şüphelenen herhangi bir Getinge çalışanının konuşması ve konuyu bölüm yöneticilerine, Etik ve Uyum Ofisine veya Getinge Speak Up Hattını kullanması beklenir. Getinge Speak Up Line, Getinge dahili ve harici web sayfalarında mevcuttur. Getinge'de, konuşan, endişelerini veya görüşlerini ifade eden birine karşı herhangi bir misilleme biçimini kabul etmiyoruz.

Daha fazla bilgi için: Global Speak Up and Non Remisilation Directive

19. Roller ve sorumluluklar

Tüm Getinge çalışanları, bu Küresel Politikayı okumaktan, anlamaktan ve bunlara uymaktan bireysel olarak sorumludur. Her çalışan, bu Küresel Politikaya uygun hareket etmekten sorumludur.

Her bölüm yöneticisi, her ekip üyesinin bu Küresel Politikaya ve ilgili Direktiflere, Talimatlara ve Yönergelere erişebildiğinden emin olmaktan sorumludur.

Veri gizliliği alanında düzenli bilgi ve eğitimin yanı sıra uyumluluk takibi de dahil olmak üzere günlük güçlendirme, her yöneticinin sorumluluğunun bir parçasıdır.

Bu Küresel Politikaya aykırı ihlaller, fesih de dahil olmak üzere disiplin cezalarına yol açabilir.

20. Rehberlik ve yardım

Getinge'nin veri gizliliği alanındaki bakış açıları söz konusu olduğunda davranışlarımıza rehberlik etmek için, bu Küresel Politika ve çeşitli direktifler ve talimatlar bulunmaktadır. Bu Küresel Politika hakkında sorularınız varsa veya hangi kuralların geçerli olduğundan emin değilseniz, lütfen Veri Gizliliği Ekibi ile iletişime geçin.

21. Faydalı linkler

Başlık
Kişisel Veri İhlali Direktifi
Veri Gizliliği Yönetişim Direktifi
Bilgi Güvenliği Direktifi
Küresel Sesini Yükselt ve Misilleme Yapmama Direktifi