QTERMINALS

VERİ KORUMA POLİTİKASI

İçindekiler

1. AMAÇ VE POLİTİKA BEYANI

Büyük hacimli verilerin hızlı değişimi, artık QTerminals'taki bizler de dahil olmak üzere modern toplumlar ve işletmeler için hayati önem taşıyor. Maalesef küreselleşen dünyada veriler sadece fırsatlar değil, aynı zamanda tehditler de yaratıyor. Bu durum özellikle Kişisel Veriler konusunda kötüye kullanımın temel hak ve özgürlüklerin ihlaline yol açabileceği durumlarda gerçekleşebiliyor.

QTerminals, Kişisel Verilerin korunmasını sosyal sorumluluğumuzun bir parçası olarak görür ve verileri sorumlu bir şekilde yönetmeye kararlıdır. Bu politikayla, QTerminals, Kişisel Verilerin yasal olarak korunmasını ve sorumlu bir şekilde işlenmesini sağlamak amacıyla işlenmesine yönelik bir çerçeve oluşturur.

2. UYGULAMA KAPSAMI

Politika küresel olarak tüm Çalışanlar için geçerlidir. Bu Politika herhangi bir ulusal veya uluslararası yasanın yerine geçmez. Mevzuatın daha sıkı standartlar veya Kişisel Verilerin daha yüksek düzeyde korunmasını gerektirmesi durumunda, bu Politikanın önüne geçmelidir.

3. TANIMLAR

Kişisel Veri, Kişisel Veri, kimliği belirli veya belirlenebilir bir gerçek kişiye ('Veri Sahibi') ilişkin her türlü bilgi anlamına gelir. Kimliği belirlenebilir gerçek kişi, doğrudan veya dolaylı olarak, özellikle isim, kimlik numarası, konum verileri gibi bir tanımlayıcıya atıfta bulunularak kimliği belirlenebilen kişidir. Ayrıca, çevrimiçi bir tanımlayıcı veya söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel veya sosyal kimliğine özgü bir veya daha fazla faktör de olabilir.

Veri Sahibi, Kişisel Verileri bu Politika kapsamında işlenen herhangi bir gerçek kişiyi ifade eder.

İşleme, otomatik araçlarla olsun ya da olmasın, Kişisel Veriler üzerinde gerçekleştirilen her türlü işlem anlamına gelir. Kişisel Verilerin toplanması, kaydedilmesi, düzenlenmesi, yapılandırılması, saklanması, uyarlanması veya değiştirilmesi, geri getirilmesi, danışılması, kullanılması, iletilerek açıklanması, dağıtılması veya başka şekilde kullanılabilir hale getirilmesi, hizalanması veya birleştirilmesi, kısıtlanması, silinmesi veya imha edilmesi gibidir.

Kontrolör, yetkili Çalışan anlamına gelir. Bu Çalışan, Kişisel Verilerin İşlenme amaçlarını ve araçlarını tek başına veya başkalarıyla birlikte belirleyebilir. Örneğin, iş sözleşmesinin işlenmesinden sorumlu olan bir İK koordinatörü.

Onay, Veri Sahibinin kendisiyle ilgili Kişisel Verilerin İşlenmesini kabul etme isteğinin serbestçe verilmiş, spesifik, bilgilendirilmiş ve net bir şekilde belirtilmesi anlamına gelir.

Çalışanlar, tüm QTerminals çalışanları (sözleşmeli çalışanlar dahil), memurlar ve direktörler anlamına gelir.

Etik İnceleme Paneli (EİP), QTerminals bünyesinde rapor edilen tüm etik dışı konular, suiistimaller ve suiistimalleri zamanında incelemeyi ve ilgili disiplin cezasına karar vermeyi taahhüt eden çok disiplinli bir kuruluş anlamına gelir. EİP üyeleri, iddia edilen suiistimal veya yanlış davranışın niteliğine ve ciddiyetine bağlı olarak Grup Hukuk ve Uyumluluk Direktörü tarafından vaka bazında seçilir.

Bölüm Yöneticisi, belirli bir Çalışanın doğrudan yönetim sorumluluğuna sahip olan kişidir.

Kişisel Veri İhlali, Kişisel Verilerin kazara veya yasa dışı imhasına, kaybına, değiştirilmesine, izinsiz ifşa edilmesine veya kişisel verilere erişilmesine yol açan bir güvenlik ihlali anlamına gelir.

QTerminals, Qterminals W.L.L. ve kontrol edilen bağlı ortaklıkları, bağlı ortaklıkları ve ortak girişimleri anlamına gelir.

4. İLKELER

Kişisel Verilerin İşlenmesinde, aşağıda belirtilen temel ilkeleri takip ediyoruz:

- **Yasallık**: Kişisel Veriler, yalnızca yeterli yasal temele dayalı olarak toplanmalı ve işlenmelidir.
- **Adillik ve Şeffaflık**: Kişisel Veriler dikkatle kullanılmalıdır. Bununla birlikte, Veri Sahipleri, Kişisel Verilerinin nasıl ve hangi amaçla yönetildiğini anlaşılır, kolay erişilebilir ve açık bir şekilde bilmelidir.
- **Amaç Sınırlaması**: Kişisel Veriler, yalnızca Kişisel Verilerin toplanması sırasında açıkça açıklanan meşru amaçlarla işlenmelidir. Kişisel Veriler bu amaçlarla bağdaşmayacak şekilde işlenemez.
- **Veri Minimizasyonu**: Kişisel Verilerin Toplanması ve İşlenmesi, tanımlanan meşru amaçlar için kesinlikle gerekli olanlarla sınırlı olmalıdır.
- **Depolama Sınırlaması**: Kişisel Veriler, verinin işlenme amacına ulaşmak için gereken süreden daha uzun süre saklanmamalıdır.
- **Doğruluk**: Kişisel Veriler doğru ve güncel olmalıdır. Yanlış verileri silmek veya düzeltmek için makul adımlar atılmalıdır.
- **Bütünlük ve Gizlilik**: Kişisel Veriler, yetkisiz veya yasa dışı işlemeye, kazara kaybolmaya, yok edilmeye veya hasara karşı korunmalıdır. Kişisel Verilerin güvenli ve gizli bir şekilde saklanması ve işlenmesini sağlamak için uygun teknik ve organizasyonel önlemlerin alınması ve takip edilmesi gerekmektedir.
- **Hesap Verebilirlik**: Bu Politikanın ilke ve hükümlerine bağlılığın sağlanması için açık yönetişim ve etkili süreçler uygulamaya konulmalıdır. Bu Politikanın gerekliliklerine uygunluğun gösterilebilmesi için ilgili kayıtlar ve belgeler muhafaza edilmelidir.
- **Erişim Kontrolü**: Kişisel verilere erişim, bilinmesi gereken esasına göre olmalı ve yalnızca yetkili kişilerle sınırlandırılmalıdır.

5. VERİ TOPLAMA VE İŞLEME

Kişisel Verilerin Toplanmasına, İşlenmesine ve kullanılmasına, yürürlükteki yasalara uygun olarak yalnızca belirli koşullar altında izin verilir. Buna aşağıdakiler dahildir:

- Veri Sahibinin önceden onayı.
- Veri Sahibi ile ilgili bir sözleşmenin yerine getirilmesi.
- Yasanın getirdiği yükümlülük.
- Bireylerin önemli çıkarlarının korunması.
- Kamu yararına veya ulusal makamların işlevlerine ilişkin görevin yerine getirilmesi.
- QTerminals'ın veya üçüncü bir tarafın meşru menfaati.

Veri Sahibinin onayı ve bir sözleşmenin yerine getirilmesi, Kişisel Verilerin QTerminals'ta İşlenmesinin iki temel dayanağıdır. Verilerin Onaya dayalı olarak işlenmesi durumunda, Veri Sahibi, veri işlemeye ilişkin kısa, şeffaf, anlaşılır, kolay erişilebilir bir biçimde ve açık bir dille bilgi almalıdır. Veri Sahibi, onay vermeden önce en azından aşağıdaki konularda bilgilendirilmelidir:

- Kişisel Verilerin işlenmesinin amacı ve yasal dayanağı.
- Kişisel Verilere erişimi olacak Kontrolörlerin kimlik ve iletişim bilgileri.
- İşleme faaliyetlerinin kapsamlı ve doğru açıklaması.
- Alıcılar veya alıcılar kategorileri.
- Kişisel Verilerin saklanma süresi veya bu mümkün değilse bu sürenin belirlenmesinde kullanılan kriterler.
- Veri Sahibinin Hakları.
- Profil oluşturma da dahil olmak üzere otomatik karar verme mekanizmasının varlığı.

Etnik köken, çocuklar, sağlık, fiziksel veya psikolojik durum, dini inançlar, evlilik ilişkileri ve suçlarla ilgili Kişisel Veriler hassas olarak kabul edilir. Sorumlu Denetleyiciler, hassas Kişisel Verilerin İşlenmesiyle ilgili olarak her zaman yerel mevzuata uymalıdır.

6. VERİ SAHİBİNİN HAKLARI

Veri Sahipleri, kendi Kişisel Verileriyle ilgili olarak aşağıdaki haklara sahiptir:

- İşlemenin niteliği ve koşulları ve Veri Sahibinin bu konudaki hakları hakkında bilgi sahibi olmak.
- Kişisel Verilere erişmek ve Kişisel Verilerinin bir kopyasını almak.
- Yanlış Kişisel Verileri düzeltmek.
- Onaynın geri çekilmesi (yalnızca Kişisel Verilerin rızaya dayalı olarak işlenmesi durumunda geçerlidir).
- Yasal dayanak veya amacın geçerliliğinin sona ermesi durumunda Kişisel Verilerin silinmesini talep etmek.
- Denetleyicinin İşleme için meşru gerekçeleri olmadığı sürece İşleme'ye itiraz etmek ve İşlemeyi kısıtlamak.
- Doğrudan pazarlamaya veya otomatik profil oluşturmaya itiraz etmek ve bunlardan hariç tutulmak.
- Veri Denetleyicileri, talep edilmesi halinde Veri Sahiplerine haklarını kullanma konusunda yardımcı olmalıdır.

7. GÜVENLİK KONTROLLERİ

Kişilerin hak ve özgürlüklerine yönelik riskler dikkate alınarak Kişisel Verilerin güvenliğinin sağlanmasına yönelik teknik ve organizasyonel tedbirlerin uygulanması gerekmektedir. İşlemenin uygulama maliyeti, kapsamı ve amaçlarının yanı sıra önlemler en azından aşağıdakileri içermelidir:

- Kişisel Veriler, son kullanıcı mesajlaşma teknolojileri (ör. e-posta) aracılığıyla aktarıldığında şifrelenmelidir.
- Tanım gereği, Kişisel Veriler gizli olarak sınıflandırılmalı ve yalnızca bilinmesi gerekenler temelinde erişilmelidir.
- Kişisel Veriler yalnızca yetkili personelin erişebileceği şekilde dosyalanmalı, saklanmalı ve yalnızca korumalı iletişim araçları kullanılarak aktarılmalıdır.
- Kişisel Veriler, İşleme amacına takma ad verilen veriler kullanılarak ulaşılabiliyorsa, takma ad kullanılmalıdır.
- Kişisel Veriler, Veri Saklama Politikası'nın "İmha" bölümü doğrultusunda güvenli bir şekilde imha edilmelidir.
- Fiziksel veya teknik bir olay durumunda verilerin kullanılabilirliği zamanında yeniden sağlanmalıdır.
- Çalışanlar, Kişisel Verilerin İşlenmesine dahil olmaları durumunda veri koruma eğitimi almalıdır.

Yeni süreçler başlatırken veya mevcut süreçleri önemli ölçüde değiştirirken, Kişisel Verilere yönelik güvenlik riskleri dikkate alınmalıdır. Bu tür değişikliklerin bireylerin hak ve özgürlükleri açısından yüksek risk oluşturma ihtimalinin olması durumunda Veri Koruma Etki Değerlendirmesi yapılmalıdır. Veri Koruma Etki Değerlendirmesinin sonuçları Uyumluluk ekibi tarafından onaylanmalıdır.

Kişisel Verilerin korunmasına yönelik teknik ve organizasyonel tedbirlerin etkinliği, Uyumluluk ve İç Denetim ekipleri tarafından düzenli olarak test edilmeli ve değerlendirilmelidir.

8. İHLALLERİN BİLDİRİMİ

Kişisel Verilerin ihlalinden şüphelenilmesi durumunda uyum ekibinin derhal bilgilendirilmesi gerekmektedir. İhlalin bireyin hak ve özgürlüklerine yönelik risk oluşturmasının muhtemel olduğu durumlarda Uyum ekibi, Veri Sahibini ve denetleyici makamı ihlal konusunda bilgilendirmelidir. Denetleyici ve Uyum görevlileri, Kişisel Veri İhlaliyle ilgili gerçekleri, bunun etkilerini ve riskleri azaltmak için alınan önlemleri belgelemelidir.

Uyumluluk ekibi, Kişisel Verilerin her ihlalini araştırmalı ve daha sonraki ihlallerin etkisini önlemek veya en aza indirmek için güvenlik kontrolleri ekleme veya ayarlama ihtiyacını değerlendirmelidir.

9. VERİ AKTARIMI

Yerel mevzuattaki olası farklılıklar göz önüne alındığında, Veri Denetleyicileri Kişisel Verilerin aktarımından önce yerel yasalara danışmalı ve bunlara uymalıdır. Buna hem şirketler arası transfer hem de üçüncü bir tarafa transfer dahildir. Kişisel Veriler, yalnızca alıcıların yeterli düzeyde veri koruma kontrollerine sahip olması ve Kişisel Verileri yerel mevzuata uygun şekilde işlemesi durumunda aktarılabilir. Aktarımın bir sözleşmenin ifası için gerekli olmadığı veya kamu çıkarını ilgilendiren önemli sebepler olmadığı sürece Veri Sahibinin rızasının alınması gerekmektedir. Kişisel Verilerin, üçüncü taraflara aktarımı her zaman belirli Veri Aktarım Sözleşmesine veya Veri İşleme Sözleşmesine dayanmalıdır. Bu anlaşmalar, aktarımın yasal dayanağını belirleyecek ve veri alıcısının veri koruma standartlarına uymasını sağlayacaktır.

10. DOKÜMANTASYON

Kişisel Verilerin tüm İşleme faaliyetlerinin yazılı kaydı ilgili Kontrolör tarafından tutulmalıdır. Kayıt, Denetleyicinin iletişim bilgilerini ve Veri Sahibinin onayını (varsa) içermelidir. Buna, İşleme amaçları, Kişisel Verilerin ve Veri Sahiplerinin kategorilerinin açıklaması, verilerin açıklanacağı veya aktarılacağı alıcı kategorileri ve mümkünse Kişisel Verilerin saklanmasına ilişkin zaman sınırları ve uygulanan güvenlik önlemleri dahildir.

11. SORUMLULUKLAR

Tüm Çalışanlar bu Politikaya uymaktan sorumludur. Çalışanların bu Politikanın ve QTerminals tarafından yayınlanan tüm ek prosedürlerin tüm yönlerini okumasını, anlamasını, kabul etmesini ve bunlara uymasını bekliyoruz. Tüm Çalışanların, bu konuyla ilgili soruları açıklığa kavuşturmak, bilgi talep etmek veya endişelerini ifade etmek için Birim Yöneticileri ve gerekirse İK veya Uyumluluk Görevlisi/Temsilcisi ile iletişime geçmesi teşvik edilir.

Tüm Birim Yöneticileri, Uyumluluk veya İK departmanlarından gelen ilgili rehberlikle birlikte, kendilerine rapor veren Çalışanların Veri Saklama ile ilgili endişelerinin çözülmesini sağlayacaktır.

QTerminals yönetimi, yasal gerekliliklere ve bu Politikanın hükümlerine uyulmasını sağlamaktan sorumludur. QTerminals'ın liman veya terminal düzeyindeki her yönetici üst düzey yöneticisi, sorumlu oldukları iş biriminin bu Politikaya tamamen uygun olduğundan ve böyle kalacağından emin olmalıdır. Ayrıca bu Politikanın farkındalığını ve anlaşılmasını teşvik etmeli ve bu Politikanın etkili bir şekilde uygulanması için yeterli kaynakların tahsisini sağlamalıdırlar. Uyumluluk ekibi özellikle bu Politikaya uyumu mümkün kılan gerekli süreçlerin mevcut olduğundan emin olmalıdır.

12. KONUŞUN

Çalışanlar, QTerminals bünyesinde veya Üçüncü Taraflardan herhangi birinde raporlama yapabilir. Çalışanlar, Bölüm Yöneticilerini, İK departmanlarını veya Uyum Görevlisini/Temsilcisini bilgilendirerek bildirimde bulunabilirler. Bunun yerine, QTerminals intranetinde, QTerminals web sitesinde ve özel bir telefon hattında bulunan QTerminals Etik Hattı aracılığıyla rapor verebilirler.

Ayrıca, Politikanın bilinen veya şüphelenilen bir ihlalini fark eden ve bildiren kişilere karşı herhangi bir misilleme yapılması kesinlikle yasaktır. İyi niyetle bir ihlali bildiren kişiye karşı misilleme yaptığı kanıtlanan herkes disiplin cezasına tabi olacaktır. Ancak, herhangi bir yanlış veya kötü niyetli iddia, iş akdinin feshine kadar varabilecek uygun disiplin ve yasal işlemlere de yol açabilir.

İhbar süreci hakkında daha fazla bilgi için lütfen QTerminals İhbar ve Dolandırıcılıkla Mücadele Prosedürlerine bakın.

13. DİSİPLİN CEZASI

QTerminals'ta, "Uygulama Kapsamı"nda belirtildiği üzere, bu Politikanın geçerli olduğu herkesin bu Politikaya uyması beklenir. Bunların herhangi bir şekilde ihlali, iş akdinin feshi veya yasal işlemler gibi disiplin cezasıyla sonuçlanabilir.

Yanlış davranışlara ilişkin şikayetlerin soruşturma gerektirmesi durumunda, sonuçları ve önerilen düzeltici eylemler Etik İnceleme Paneli (EİP) tarafından incelenecek soruşturmalar yapılacaktır. Düzeltici eylemler, davranışın ihlaline ilişkin gerçekler ve koşullar ile soruşturmanın sonuçlarına göre belirlenecektir.

Davranış Kuralları veya bu Politikanın suiistimal ve ihlal iddialarına ilişkin soruşturma süreci hakkında daha fazla bilgi için lütfen QTerminals İhbar ve Dolandırıcılıkla Mücadele Prosedürlerine bakın.

14. İNCELEME SÜRECİ

Uyumluluk ekibi, Veri Korumayla ilgili risklerin takip edilmesinden ve bu Politikanın düzenli olarak gözden geçirilmesinden, değerlendirilmesinden ve iyileştirilmesinden sorumludur. Politikanın riskleri ve genel etkinliği üst yönetime rapor edilmelidir.

Belgeyi onaylayan:

Grup İcra Kurulu Başkanı
Neville Bissett