Güvenlik Politikası

1. Önsöz
Veri işlemenin konusu, kapsamı, niteliği ve amacı, taraflar arasında akdedilen satış ve hizmet sözleşmesine dayalı iş ilişkisinden kaynaklanacak ve bu konuda önceki tüm sözleşmelerin yerini alacaktır. Bu Güvenlik Önlemleri, müşteri verilerinin işlenmesiyle ilgili olduğu ölçüde, Müşteri ile Axess arasında akdedilen satış sözleşmesini tamamlayacak ve onun ayrılmaz bir parçası olarak kabul edilecektir. Axess, Axess ile Müşteri arasındaki müşteri ilişkisi çerçevesinde aşağıdaki BT güvenlik önlemlerini garanti eder.

2. Genel teknik ve organizasyonel önlemler
Axess, aktarılan verilerin veri işleme sistemlerinde işlenmesi için her zaman GDPR uyarınca gerekli tüm önlemleri alacaktır. Dahili organizasyonun veri koruma gereksinimlerini karşılayacak şekilde tasarlanmasını sağlar. Aşağıdaki koşullar, sunucunun nerede barındırıldığına bakılmaksızın geçerlidir.

2.1 Kullanım amacı kontrolü:
Farklı amaçlarla toplanan verilerin ayrı ayrı işlenmesi aşağıdaki önlemlerle garanti edilmektedir:
> Yazılım tabanlı (örn. Müşteri ayrımı)
> Erişim düzenlemesi yoluyla ayırma (veritabanı ilkesi)
> Test ve mevcut verilerin ayrılması
> Test ve mevcut sistemlerin ayrılması (teknoloji, programlar)

2.2 Anonimleştirme
İlgili veri işleme için mümkün olduğu ölçüde, kişisel verilerin birincil tanımlama özellikleri ilgili veri uygulamasında kaldırılacak ve ayrı olarak saklanacaktır.

2.3 Giriş kontrolü:
Kişisel verilerin, veri işleme sistemlerine kim tarafından ve kimler tarafından girildiği, değiştirildiği veya veri işleme sistemlerinden çıkarılıp çıkarılmadığının daha sonra kontrol edilip belirlenebileceği garanti edilmektedir. Axess bu amaçla girişleri/günlük dosyalarını belgeleyecek veya kaydedecektir.

2.4 Tasarıma Göre Gizlilik ve Varsayılan Gizlilik
Teknik ve organizasyonel önlemlerin bir parçası olarak uygun varsayılan ayarlar, prensip olarak, yalnızca belirtilen işleme amacı için işlenmesi gerekli olan kişisel verilerin işlenmesini sağlar.
> örn . sezon biletleri, vb.) işlenmesi için gerekli olması halinde toplanacaktır .
> Axess web mağazalarında çerezlerin ayarlanması ancak kullanıcının onayı ile mümkündür.
> Kişisel verilerin pazarlama amaçlı kullanımına yalnızca kullanıcının aktif onayı ile izin verilir.

3 Axess tarafından sunucu barındırma durumunda teknik ve organizasyonel önlemler
Müşterinin Axess VERİ MERKEZİ HİZMETİ kullanması durumunda, güvenlik alanlarının ve yetkili kişilerin çemberinin veya erişim yetkilerinin tanımlanması, erişim yollarının uygun şekilde güvence altına alınması ve veri taşıyıcılarının güvenli bir şekilde kontrol edilmesi ve saklanması sağlanır. Aşağıdaki önlemler yalnızca sunucu Axess tarafından barındırılıyorsa geçerlidir.

3.1 Giriş denetimi:
Yetkisiz kişilerin, verilerin işlendiği veya kullanıldığı veri işleme sistemlerine girmesi yasaktır. Bilgisayar odaları , depreme dayanıklı olarak sınıflandırılan bir ofis binasında yer almaktadır . Tesise yalnızca BT, Tesis ve Yönetim çalışanları erişebilir. Erişim kontrolü aşağıdaki önlemlerle sağlanır:
> Yetkilendirme-/Chipcard

Güvenlik bölgesindeki mevcudiyet kaydedilir. Yetkili olmayan personel ve şirkete ait olmayan kişiler (servis teknisyenleri, danışmanlar, temizlik personeli vb.) ancak yetkili kişiler eşliğinde odalara girebilir. Kabul kontrolü, aşağıdaki ilave organizasyonel/teknik önlemlerle desteklenir:
> Alarm sistemi
> Bina gözetimi
> Video teknolojisi

3.2 Giriş kontrolü:
Veri işleme sistemlerinin yetkisiz kişiler tarafından kullanılması aşağıdaki önlemlerle engellenmektedir:
> Şifre

Her yetkili kişinin yalnızca kendisinin bildiği ve düzenli aralıklarla değiştirilmesi gereken kendi şifresi vardır. Veri işleme ve telekomünikasyon sistemindeki tüm faaliyetlerle ilgili otomatik protokoller (Log dosyaları) oluşturulur. Veri işleme sistemlerinin yetkisiz kişiler tarafından veri iletimi için ekipman yardımıyla kullanılması aşağıdaki önlemlerle engellenir:
> VPN (Sanal Özel Ağ)

3.3 Giriş kontrolu:
Bir veri işleme sistemini kullanmaya yetkili kişilerin, erişim yetkisine tabi verilerine münhasıran erişebilecekleri ve verilerin işlenmesi, kullanılması ve saklanması sırasında yetkisiz olarak okunamayacağı, kopyalanamayacağı, değiştirilemeyeceği ve silinemeyeceği garanti edilmektedir. Yetkili kişinin erişim yetkisine tabi verilere münhasıran erişim olanağının kısıtlanması, aşağıdaki önlemlerle garanti edilir:
> Erişim yetkisinin otomatik olarak incelenmesi (sistemde)

3.4 Aktarım kontrolü:
Kişisel verilerin elektronik ortamda iletilmesi veya taşınması sırasında veya veri taşıyıcılarında saklanması sırasında izinsiz olarak okunamayacağı, kopyalanamayacağı, değiştirilemeyeceği, kaldırılamayacağı ve kontrol edilip belirlenebileceği, kişisel verilerin aktarımının hangi noktada gerçekleştirildiği garanti edilmektedir. veri aktarım cihazları tarafından öngörülmüştür. Veri taşıyıcılarının sevkiyatı, kayıt ve beraberindeki belgelerle belgelenir ve kontrol edilir. Odalara özel veri taşıyıcılarının getirilmesi ve kullanılması yasaktır. Veri taşıyıcıları aşağıdaki şekilde imha edilir:
> Manyetik veri taşıyıcıları üzerine yazma ve fiziksel imha yoluyla (harici servis sağlayıcı tarafından yapılmaktadır)
Kişisel verileri iletmek için internet kullanıldığı sürece, aşağıdaki güvenlik önlemleri kullanılacaktır:
> Güvenlik duvarı
> Sanal Özel Ağ (VPN)

3.5 Kullanılabilirlik kontrolü:
Kişisel verilerin kazara yok edilmeye veya kaybolmaya karşı korunması aşağıdaki önlemlerle garanti edilmektedir:
> Günlük/haftalık/aylık/yıllık veri yedekleme
> Depolama Alanı Ağı (SAN)
> Disk yansıtma (diğerlerinin yanı sıra RAID)
> Kesintisiz güç kaynağı (UPS)
> Aşırı gerilim filtresi
> Acil durum jeneratörü
> Verilerin dış kaynak kullanımı
> Yangın önleme cihazları

3.6 Veri koruma yönetimi
Bir veri koruma yönetiminin kurulması ve uygulanması sağlanır. Veri koruma yönetimi aşağıdaki noktalara ayrılmıştır:
> İşleme faaliyetlerinin listesi
> Sözleşme verilerinin işlenmesi
> Veri koruma etki değerlendirmesi
> Olay yanıt yönetimi
> Veri koruma ihlalleri raporu
> Eğitim
> PDCA (Planla, Yap, Kontrol Et, Önlem Al): düzenli kontroller

3.7 Olay yanıt yönetimi
Muhtemel senaryolara karşı sorumluların nasıl tepki vermesi gerektiğine ilişkin tedbirler alındı. Bunlara veri güvenliği ihlalleri, DoS (Denial of Service), DDoS (Distributed Denial of Service), güvenlik duvarındaki boşluklar, virüs veya kötü amaçlı yazılım salgınları ve içeriden gelen tehditler dahildir.
Olay müdahale yönetimi altı önemli aşamaya ayrılmıştır:
> Hazırlık : Hem kullanıcılar hem de BT çalışanları, olası olayların meydana geldiği ve hangi adımların başlatılması gerektiği konusunda eğitilir veya bilgilendirilir.
> Tanımlama : Bir olayın bir veri koruma olayıyla ilgili olup olmadığının belirlenmesi.
> Muhafaza : Olayın neden olduğu zararları sınırlamak ve daha fazla zararı önlemek için etkilenen sistemleri izole etmek.
> Eradikasyon : Olayın nedenini veya neyin tetiklediğini bulmak ve etkilenen sistemleri üretken ortamdan çıkarmak.
> Kurtarma : Daha fazla tehdidin bulunmadığından emin olduktan sonra, etkilenen sistemleri tekrar üretken ortama entegre etmek.
> Kazanılan bilgi: Olay belgelerinin tamamlanması ve ekibin veya şirketin olaydan neler öğrenebileceğinin analizi. Bu şekilde, belirli koşullar altında gelecekteki yanıtlar geliştirilebilir.

4 Müşteri Verilerine Erişim
Axess, sorun olması durumunda yeterli desteği verebilmek için, Axess ile Müşteri arasındaki satış sözleşmesi kapsamında olması veya Müşteri'nin bu erişimin Axess ile Müşteri arasındaki satış sözleşmesi kapsamında olması kaydıyla, veri işleyici olarak Müşteri sistemine veya verilerine erişme hakkını saklı tutar. Bu erişime izin vermiş müşteri veya bayi istenen hizmet talebini müşteri adına Axess'e iletmiştir. Axess şunları garanti eder:
> Merkezi donanıma herhangi bir fiziksel erişim, yalnızca müşterinin Veri Merkezi Hizmetini Axess'ten alması durumunda gerçekleşir;
> Yalnızca yukarıda açıklanan durumda ve Bayi ve/veya Müşteri'nin rızasıyla veya onun adına uzaktan bakım aracı aracılığıyla Müşteri verilerine erişim;
> Yerel cihazlara erişim, yalnızca müşterinin veya satıcının talebi üzerine destek olması durumunda verilir.

5 Sipariş düzenleme:
Mevcut iş ilişkisine ek olarak, görevlendirilmiş işlemeye ilişkin bu hükümler, Genel Veri Koruma Yönetmeliği ("GDPR") kapsamındaki tüm karşılıklı yükümlülüklerin yerine getirilmesini sağlar.

Axess, kişisel verileri Müşteri adına işler, burada konu, kapsam, tür, işlenen veri kategorileri, işlenme amacı ve veri sahibi kategorileri (Müşteri Verileri), taraflar arasında akdedilen ilgili satış sözleşmesinden kaynaklanır. sözleşme tarafları. Bu nedenle, görevlendirilen işlemeye ilişkin bu hükümler, kişisel verilerin işlenmesiyle ilgili oldukları ölçüde, Müşteri ile Axess arasında akdedilen tüm sözleşmeleri tamamlar.

Güvenlik Politikası

Axess tarafından veri işleme, münhasıran Avrupa Birliği'nin bir Üye Devletinde gerçekleştirilecektir, bu sayede Madde 4 satır 23 GDPR (Birlik içinde) uyarınca sınır ötesi veri işleme, sorumlu taraf olarak Müşteriye, Müşterinin itiraz edebilmesi için işlemin başlamasından önceki son süre. Bu bildirime sessiz kalmak, işlemeye onay vermek anlamına gelir.

5.1 İşlemcinin Yükümlülükleri:
Müşteri, satın alma sözleşmesini imzalayarak bu politikada belirtilen teknik ve organizasyonel önlemleri kabul etmiş olur. Axess, bu politikayı uygulayarak ve müşterinin kişisel verilerle ilgili genel ve bireysel talimatlarına uyarak (örn . her türlü sadece bir ihlal durumunda yapılabilir.), Axess sözleşmeye dayalı veri uygulamalarının en gelişmiş düzeyde korunmasını sağlar, böylece her türlü iddia ancak bir ihlal durumunda yapılabilir.

İşlenen kişisel veriler için tutarlı bir koruma seviyesi sağlayan veya bu seviyeyi artıran teknik ve organizasyonel önlemlerde yapılan değişiklikler onaylanmış sayılacak ve talep üzerine Müşteriye açıklanacak, ancak Axess tarafından Müşteriye açıklanması gerekmeyecektir.

Axess, Müşterinin GDPR Bölüm III kapsamındaki veri sahiplerinin haklarına (bilgi, erişim, düzeltme, silme, kısıtlama, veri taşınabilirliği, itiraz ve otomatik karar verme) uymasını sağlamak için yasal zaman sınırları içinde yukarıda açıklanan teknik ve organizasyonel önlemleri alacaktır.

5.2 Veri işleme
Axess, kişisel verileri yalnızca mevcut sözleşmeler çerçevesinde ve müşterinin bireysel talimatlarına uygun olarak işlemeyi taahhüt eder. Axess, verileri kanunen üçüncü şahıslara vermek zorundaysa, Axess, müşteriyi, verilerin ifşa edilmesinin yasal yükümlülüğü hakkında bilgilendirecektir. Sözleşme ilişkisi dışındaki amaçlar için başka herhangi bir veri aktarımı, yalnızca müşterinin yazılı bir siparişe dayalı talimatı üzerine gerçekleşir.

Axess, veri işleme ile görevlendirilen tüm kişilerin, faaliyetlerine başlamadan önce - faaliyetleri sona erdikten sonra bile gizlilik yürürlükte kalacak şekilde - gizliliğe bağlı olmalarını veya uygun bir yasal gizlilik yükümlülüğüne tabi olmalarını sağlayacaktır.

5.3 Bilgilendirme görevi
Axess, GDPR'nin 32 ila 36. Maddelerinde belirtilen yükümlülüklere uyma konusunda Müşteriye yardımcı olacaktır (işleme güvenliği, kişisel veri ihlallerinin denetim makamına bildirimi, kişisel veri ihlalinden etkilenen kişinin bildirimi, veri koruma etki değerlendirmesi, danışma)

Axess, talep üzerine, GDPR'nin 28. Maddesinde belirtilen yükümlülüklere (İşleyicinin yükümlülükleri) uygunluğu göstermek için Müşteriye gerekli tüm bilgileri (örn. mevcut sertifikalar, teknik ve organizasyonel önlemler, vb.) sağlayacaktır. Ayrıca, Axess, Müşteri veya Müşteri tarafından atanan başka bir denetçi tarafından gerçekleştirilen denetimlere - teftişler dahil - olanak sağlayacak ve katkıda bulunacaktır.

Axess, GDPR'nin ihlali durumunda veya Axess'in Müşteri'nin bir talimatının Birlik veya Üye Devletlerin veri koruma hükümlerini ihlal ettiğine inanması durumunda, Müşteri'yi gereksiz gecikme olmaksızın bilgilendirecektir.

5.4 Sipariş kontrolü
Müşteri adına işlenen kişisel verilerin sadece müşterinin talimatlarına uygun olarak işlenmesi sağlanır. Axess, aşağıdaki görevlendirilmiş veri işleme türleri için harici taraflarla sözleşmeler yürütür:
> Harici taraflarca veri işleme
> Veri ortamı imhası / harici taraflarca imha edilmesi
> Harici taraflarca bakım ve uzaktan bakım
> Harici taraflarca yönetim / uzaktan yönetim

Kişisel verilerin müşteri adına işlenmesi - yalnızca müşterinin talimatlarına uygun olarak - aşağıdaki önlemlerle garanti edilir.
> Yazılı talimatlar
> Teklif ve sipariş onayı
> takma ad

5.5 Alt işlemciler
Axess, kişisel verilerin işlenmesi için alt işlemciler kullanmaya yetkilidir. Alt işleyici ile ilgili olarak amaçlanan değişiklikler , Müşteri'nin değişikliğe itiraz edebilmesi için yeterli bir süre içinde Müşteri'ye yazılı olarak bildirilecektir. Bildirimin mümkün olmadığı veya uygulanabilir olmadığı durumlar (özellikle yakın tehlike durumunda) bu kuralın dışındadır. Axess, alt işlemcilerle yazılı bir sözleşme akdeder ve onlarla, gerekli değişiklikler yapılarak, bu bölümde sunulanlarla aynı veri koruma kanunu yükümlülüklerini kabul eder.
Aşağıdaki alt işlemciler Axess tarafından sözleşmeye tabidir:
https://teamaxess.com/en/security-policy-sub-processors
Axess'in resmi bir bayisi ile bir satın alma sözleşmesi yapılması durumunda, Axess verileri yalnızca ilgili yükleniciye (ortak veya bayi) iletecektir.

6 Sözleşme sonunda sözleşme verilerinin işlenmesi
Temel iş ilişkilerinin sona ermesi üzerine, Axess, Kişisel Verileri Birlik veya Üye Devlet yasaları uyarınca saklama yükümlülüğü bulunmadığı sürece, tüm Kişisel Verileri veri işleme için alışılmış bir formatta Müşteriye iade edecek veya silecektir.

7 Nihai hükümler
Güvenlik Politikası, Axess ile Müşteri arasındaki iş ilişkisinin süresi ile aynı süreye sahip olacaktır. Aynısının nihai hükümleri, sipariş işleme sözleşmesine uygun olarak uygulanacaktır.