GÜVENLİK POLİTİKASI

EKİP MÜHENDİSLİK MAKİNA DAYANIKLI TÜKETİM MALLARI İLETİŞİM İNŞAAT DIŞ TİCARET SAN.VE TİC. A.Ş.' in güvenlik anlayışı, müşteri memnuniyeti ve güvenliği odaklı hizmet felsefesi ile Online işlemleri gereği, web sitesi www.ekiptermo.com adresine (bundan sonra "Web Sitesi" olarak ifade edilecektir.) ve tarafımızdan geliştirilen yazılımlar için vermiş olduğunuz bilgilerin emniyeti için her türlü önlem alınmıştır. Müşterilerimizin rahatça ve güvenli bir şekilde Web Sitemiz ve yazılım programlarımızı kullanmaları, hizmetleri incelemeleri, sipariş verebilmeleri ve hizmet ödemesi yapabilmeleri için tüm gerekli altyapı sağlanmıştır. Şirketimizin Güvenlik Politikası gereği; Müşterilerimizin güvenli bir şekilde, rahatça alışveriş yapabilmelerini ve hizmet alabilmelerini sağlamak için en gelişmiş güvenlik sistemlerini kullanmaktadır

Sistemimizdeki 256 bit SSL sayesinde üyelik bilgileriniz üçüncü şahısların gözünden ve müdahalesinden korunmaktadır. Üyelik işlemlerinin bütün aşamasında tüm bilgi alışverişi SSL güvencesi altındadır ve tüm veri akışı şifreli olarak yapılmaktadır. Bu, pratik olarak kırılması mümkün olmayan bir şifrelemedir. SSL güvenlik protokolü sayesinde müşterilerimizin Web Sitemize verilen tüm bilgiler şifrelenerek direkt olarak bankaya veya ilgili sanal pos hizmeti alınan kuruluş üzerinden bankaya gönderilir ve bu işlem sırasında bu bilgilere **EKİP MÜHENDİSLİK MAKİNA DAYANIKLI TÜKETİM MALLARI İLETİŞİM İNŞAAT DIŞ TİCARET SAN.VE TİC.A.Ş.** personeli dahi ulaşabilmesi mümkün değildir. Sistemimiz üzerinden yapılan online ödemelerde müşterilerimizin kart bilgileri sistemimizde kaydedilmemektedir. Kart bilgileri uygulama üzerinden anonimleştirilerek alınmaktadır. Ödeme sonrasında bilgiler ya direkt olarak bankaya ya da ilgili sanal pos hizmeti alınan kuruluş tarafından bankaya aktarılmaktadır. Bu süreçte sistemimiz üzerinden yapılan veri aktarımına dair kişinin ad-soyadı ile işlem kaydı eşleştirilmekte olup, ödeme bilgileri sistemde kaydedilmemektedir. Bu kapsamda, EKİP MÜHENDİSLİK MAKİNA DAYANIKLI TÜKETİM MALLARI İLETİŞİM İNŞAAT DIŞ TİCARET SAN.VE TİC.A.Ş. adına ilgili sanal pos hizmeti alınan kuruluş üzerinden, 3.şahıslara ödeme yapılması aşamasında; müşterilerimizin yaptıkları online tahsilatların yönlendirmeleri ve sair nedenler ile açığa çıkacak tüm anlaşmazlıklardan doğan bütün yasal yükümlülükleri, açığa çıkacak bütün mali ve hukuki tüm sorumlulukları peşinen kabul etmiş sayılır.

www.ekiptermo.com hiçbir müşterisinin şifre bilgilerini sisteminde saklamamaktadır. Sistemimizdeki cookie uygulamaları sayesinde; müşterilerimizin kişisel kayıt bilgilerini tekrar tekrar girmelerine gerek bulunmamaktadır.

Müşterilerimiz için oluşturduğumuz kullanıcı adı ve şifreler jenerik olarak karmaşık şifre güvenliği talimatlarına uygun oluşturulmaktadır ve şirket sunucularımızda tutulmamaktadır

Web Sitemiz ve yazılım programlarımız üzerinden **EKİP MÜHENDİSLİK tarafından** sunulan hizmetlerde oluşabilecek güvenlik aksaklıkları **EKİP MÜHENDİSLİK** kendisinden kaynaklanır ise, sorumluluğu kabul eder. 3. şahıslardan kaynaklanan güvenlik problemlerinden sorumlu tutulamaz. Bu sebeple kişisel önem arz eden veriler, şifreler ve kişisel/kurumsal değer içeren materyaller konusunda sorumluluk müşteriye aittir.

GİZLİLİK POLİTİKASI

EKİP MÜHENDİSLİK verileriniz ve kişisel bilgilerinizin gizliliğine saygı duyar. Kişisel bilgiler, 6698 sayılı Kişisel Verilerin Korunması Kanunu'na tabidir. Bu doğrultuda, yazılım programlarımız kapsamında verdiğiniz tüm kişisel bilgiler ve veriler yalnızca size hizmet amaçlı ve Kanun'a uygun olarak kullanılmakta ve hiçbir şekilde üçüncü taraf kurum ve kuruluşlarla paylaşılmamaktadır. **EKİP MÜHENDİSLİK** yazılım programlarımızdan kişisel

bilgi toplama ve kullanımını asgari düzeyde tutmakta ve toplanan kişisel bilgileri sadece işlemlerin gerçekleşebilmesi için kullanmaktadır.

EKİP MÜHENDİSLİK faaliyetleri esnasında hizmet vermekte olduğu müşterilerinin özel erişim/bağlantı bilgilerine, kritik cihazlara ait özel konfigürasyon ve iletişim bilgilerine sahip olabilmektedir. Hizmet verilen kurum ve kuruluşların güvenliğini temin etmek ve verdiğimiz hizmetler için kullandığımız bilgi varlıklarımızın güvenliğini sağlamamız öncelikli amacımızdır. Bu bağlamda; iş birliğinde bulunduğumuz müşteriler, resmi ve özel kurumlar ile ilişkilerimiz çok değerlidir. Sunmakta olduğumuz hizmetlerin sürekliliği, elimizde tuttuğumuz bilgilerin gizliliği, müşterilerin veya kendi içimizdeki bilgi varlıklarının bütünlüğü yüksek öneme sahiptir. **EKİP MÜHENDİSLİK,** olarak iç ve dış paydaşlarımızın karşılaşabileceği her türlü bilgi güvenliği riskini önlemek ve yönetmek amacıyla bir Bilgi Güvenliği Politikası hazırlanmıştır.

1. **Kişisel verilerin korunması**

EKİP MÜHENDİSLİK 6698 sayılı Kişisel Verilerin Korunması Kanunu ve kişisel verilerin korunmasına ilişkin diğer mevzuat hükümleri doğrultusunda veri sorumlusu sıfatıyla hareket etmektedir. Bu kapsamda kişisel veriler yalnızca **EKİP MÜHENDİSLİK kapsamındaki** hizmetleri ve her türlü gizlilik güvenlik prosedürünü uygulamaya yetkili **EKİP MÜHENDİSLİK personeli**, gizlilik güvenlik yetki matrislerinde adı geçen personel ve **EKİP MÜHENDİSLİK** veri sahiplerini bilgilendirme şartını sağlayarak bu hususta yetki verdiği gerçek/tüzel kişiler tarafından işleme tabi tutulur. Detaylar için lütfen "Kişisel Verilerin Korunması ve İşlenmesine İlişkin Aydınlatma Metni" linkini tıklayınız.

2. **Elektronik iletiler**

Elektronik iletiler ile ilgili olarak bizimle iletişim kurmanız sırasında ve diğer her türlü **EKİP MÜHENDİSLİK mecrasında** vermiş olduğunuz iletişim izinleri çerçevesinde iletişim bilgileriniz üzerinden **EKİP MÜHENDİSLİK ve** iş ortakları tarafından sunulan hizmetlerinin tanıtımı, yeni ürün ve hizmetler hakkında bilgiler, mevzuat duyuruları ve ilgi çekici bulacağınız diğer konular hakkında elektronik iletiler almayı kabul etmiş olursunuz. Bu kapsamda tarafınıza gönderilen iletilerin bir veya birden fazla iletişim kanalı üzerinden iletiminin durdurulması talebinizi **EKİP MÜHENDİSLİK** 'e iletebilirsiniz.

3. **Log verileri, çerezler (cookies) ve web işaretçileri**

Cookie'ler çeşitli verileri toplayan laptop, pc ve mobil cihazınızda bulunabilecek program parçacıklarıdır çerezler genellikle text dosyalardır.
Bu programlar sayesinde aşağıdaki veriler toplanabilir:

- Internet Protokolü (IP) adresi
- Siteye bağlandığınız bilgisayarın domain adı
- Bağlandığınız tarih, saat ve sitede geçirdiğiniz süre
- Bilgisayarınız hakkındaki bilgiler, tarayıcınızın markası, işletim sisteminiz, Java desteği, flash versiyonu, ekran çözünürlüğünüz ve bağlantı hızınız gibi bilgiler
- Firmamız sitesinden istek yapılırken bağlanan bilgisayardaki sayfa bilgileri
- Firmamız sitesinde transfer edilen verinin byte olarak miktarı
- İz bırakan çerezlerin içerikleri
- Yazılımlar ve self-service uygulamalar ("Uygulamalar") için gerekli olan Login zamanı, Kullanıcı Adı, Kullanıcı ID gibi alanlar
- Uygulamalar üzerinde Kullanıcının son istek yaptığı URL bilgisi
- Tarayıcınıza ait dil bilgisi

4. **Verilerinizin kullanım amaçları**

EKİP MÜHENDİSLİK e ait web sitesini ziyaretiniz sırasında otomatik olan veya olmayan yöntemlerle kaydedilen ve iletişim formu, e-posta ve diğer elektronik işlemlerle **EKİP MÜHENDİSLİK paylaştığınız** kişisel verileriniz, öncelikle taleplerinizin yerine getirilmesini sağlamak ve daha sonra ise size daha iyi hizmet sunmak amacıyla kullanılacaktır. Genel olarak kullanım amaçları aşağıdaki gibidir:

- Tarafınızla iletişime geçmek
- Tarafınızdan gelen bir soruyu yanıtlamak
- Sitemizin yönetimini sağlamak
- Hizmet kalitemizi yükseltmek

Şirket tarafından yukarıdaki amaçlarla toplanmasını istemediğiniz verilerinizi lütfen paylaşmayınız. Bu bilgileri sağlamadığınız durumda sizinle iletişimde olamayacağımızı, diğer taraftan bu siteyi ziyaretiniz ile çerezler vasıtası ile bazı verilerinizin toplanabileceğini unutmayınız.

5. **Veri güvenliği**

EKİP MÜHENDİSLİK bilgilerinizin gizliliğinin korunmasına önem vermektedir ve veri güvenliğine ilişkin gerekli tüm tedbirleri almaktadır. Bununla birlikte, internet üzerindeki bilgi alışverişleri genel anlamda çok güvenli değildir. Bu nedenle Şirket'in web sitesi üzerinden bilgi alışverişlerinizde kullanıcı olarak gerekli özeni göstermenizi tavsiye ederiz. Bu özeni göstermediğiniz taktirde, **EKİP MÜHENDİSLİK size** site içindeki iletişiminizin, kişisel ve diğer bilgilerinizin güvenliğine ilişkin veya 3. kişiler tarafından bilgilerinizin ele geçirilmesine karşı teminat veremez.
Söz konusu bilgiler **EKİP MÜHENDİSLİK 'e** ulaştığında, bu bilgiler güvenlik ve gizlilik standartlarına uygun olarak korunmaktadır.
Verileriniz, yukarıda sayılan amaçlarla ve ancak iş sürecimizin ihtiyaçları veya yasal zorunluluklar için gerekli oldukları sürece saklanmaktadır.

5.1.Siber Güvenliğin Sağlanması,

Kişisel veri içeren bilgi teknoloji sistemlerimiz internet üzerinden gelen izinsiz erişim tehditlerine karşı korunmasında alınabilecek öncelikli tedbirler, güvenlik duvarı ve ağ geçididir. Bunlar, internet gibi ortamlardan gelen saldırılara karşı ilk savunma hattıdır
Bununla birlikte hemen hemen her yazılım ve donanımın bir takım kurulum ve yapılandırma işlemlerine tabi tutulmaktadır. Ancak yaygın şekilde kullanılan bazı yazılımların özellikle eski sürümlerinin belgelenmiş güvenlik açıkları bulunmakta olup, kullanılmayan yazılım ve servislerin cihazlardan kaldırılması potansiyel güvenlik açıklarının azalmasını sağlamaya yardımcı olmayı hedeflemekteyiz. Bu nedenle, kullanılmayan yazılım ve servislerin güncel tutulması yerine silinmesi, kolaylığı nedeniyle öncelikle tercih edilebilecek bir yöntemdir.
Yama yönetimi ve yazılım güncellemeleri olup yazılım ve donanımların düzgün bir şekilde çalışması ve sistemler için alınan güvenlik tedbirlerinin yeterli olup olmadığının düzenli olarak kontrol etmekteyiz ve olası güvenlik açıklarının kapatılması için gerekli çalışmaları takip etmekteyiz.
Kişisel veri içeren sistemlere erişimlerimiz sınırlıdır. Bu kapsamda çalışanlara, yapmakta oldukları iş ve görevler ile yetki ve sorumlulukları için gerekli olduğu ölçüde erişim yetkisi tanınmalı ve kullanıcı adı ve şifre kullanılmak suretiyle ilgili sistemlere erişim sağlanmaktadır. Söz konusu şifre ve parolalar oluşturulurken, kişisel bilgilerle ilişkili ve kolay tahmin edilecek rakam ya da harf dizileri yerine büyük küçük harf, rakam ve sembollerden oluşacak kombinasyonların tercih edilmesi sağlanmaktadır. Buna bağlı olarak veri sorumlularının, erişim yetki ve kontrol matrisi oluşturulmuş ve ayrı bir erişim politika ve prosedürleri oluşturarak veri sorumlusu organizasyonu içinde bu politika ve prosedürlerin uygulamaya alınmıştır.
Güçlü şifre ve parola kullanımının yanı sıra, kaba kuvvet algoritması (BFA) kullanımı gibi yaygın saldırılardan korunmak için şifre girişi deneme sayısının sınırlandırılması, düzenli aralıklarla şifre ve parolaların değiştirilmesinin sağlanması, yönetici hesabı ve admin yetkisinin sadece ihtiyaç olduğu durumlarda kullanılması için açılması ve veri sorumlusuyla ilişikleri kesilen çalışanlar için zaman kaybetmeksizin hesabın silinmesi ya da girişlerin kapatılması gibi yöntemlerle erişimler sınırlandırılmıştır.
Kötü amaçlı yazılımlardan korunmak için ayrıca, bilgi sistem ağını düzenli olarak tarayan ve tehlikeleri tespit eden antivirüs, antispam gibi ürünlerin kullanılmaktadır. Ancak bu ürünlerin sadece kurulumu yeterli olmayıp güncel tutulmakta gereken dosyalar düzenli olarak taranmaktadır.

Veri sorumlusu olarak, farklı internet siteleri ve/veya mobil uygulama kanallarından kişisel veri temin edilecekse, bağlantıların SSL ya da daha güvenli bir yol ile gerçekleştirilmesi de kişisel veri güvenliğinin sağlanmaktadır.

5.2. Kişisel Veri Güvenliğinin Takibi

Veri sorumlularının sistemleri çoğunlukla hem içeriden hem de dışarıdan gelen saldırılar ve siber suçlara veya kötü amaçlı yazılımlara maruz kalmakta olup çeşitli belirtilere rağmen bu durum uzun süre fark edilememekte ve müdahale için geç kalınabilmektedir. Bu durumun önüne geçebilmek için;

a) Bilişim ağlarında hangi yazılım ve servislerin çalıştığının kontrol edilmesi,
b) Bilişim ağlarında sızma veya olmaması gereken bir hareket olup olmadığının belirlenmesi,
c) Tüm kullanıcıların işlem hareketleri kaydının düzenli olarak tutulması (log kayıtları gibi),
ç) Güvenlik sorunlarının mümkün olduğunca hızlı bir şekilde raporlanması,
d) Çalışanların sistem ve servislerdeki güvenlik zaafiyetlerini ya da bunları kullanan tehditleri bildirmesi için resmi bir raporlama prosedürü oluşturulması gerekmektedir. Söz konusu raporlama sürecinde oluşturulacak raporlar, sistem tarafından oluşturulacak otomatik raporlar olabilir. Bu raporların sistem yöneticisi tarafından en kısa sürede toplulaştırılarak veri sorumlusuna sunulması gerekmektedir. güvenlik yazılımı mesajları, erişim kontrolü kayıtları ve diğer raporlama araçlarının düzenli olarak kontrol edilmesi, bu sistemlerden gelen uyarılar üzerine harekete geçilmesi, bilişim sistemlerinin bilinen zaafiyetlere karşı korunması için düzenli olarak zaafiyet taramaları ve sızma testlerinin yapılması ile ortaya çıkan güvenlik açıklarına dair testlerin sonucuna göre değerlendirmeler yapılması,

Bilişim sisteminin çökmesi, kötü niyetli yazılım, servis dışı bırakma saldırısı, eksik veya hatalı veri girişi, gizlilik ve bütünlüğü bozan ihlaller, bilişim sisteminin kötüye kullanılması gibi istenmeyen olaylarda deliller toplanmalı ve güvenli bir şekilde saklanması gerekmektedir.

5.3. Kişisel Veri İçeren Ortamların Güvenliğinin Sağlanması

Kişisel veriler, veri sorumlularının yerleşkelerinde yer alan cihazlarda ya da kağıt ortamında saklanıyor ise, bu cihazların ve kağıtların çalınması veya kaybolması gibi tehditlere karşı fiziksel güvenlik önlemlerinin alınmaktadır. Aynı şekilde, kişisel verilerin yer aldığı fiziksel ortamların dış risklere (yangın, sel vb.) karşı uygun yöntemlerle korunması ve bu ortamlara giriş / çıkışların kontrol altına alınmaktadır.

Kişisel veriler elektronik ortamda ise, kişisel veri güvenliği ihlalini önlemek için ağ bileşenleri arasında erişim sınırlandırılabilir veya bileşenlerin ayrılması sağlanabilir. Örneğin kullanılmakta olan ağın sadece bu amaçla ayrılmış olan belirli bir bölümüyle sınırlandırılarak bu alanda kişisel verilerin işleniyor olması halinde, mevcut kaynaklar tüm ağ için değil de sadece bu sınırlı alanın güvenliğini sağlamak amacıyla ayrılabilecektir.Aynı seviyedeki önlemlerin veri sorumlusu yerleşkesi dışında yer alan ve veri sorumlusuna ait kişisel veri içeren kağıt ortamları, elektronik ortam ve cihazlar için de alınması gerekmektedir.

Kişisel veri güvenliği ihlalleri sıklıkla kişisel veri içeren cihazların (dizüstü bilgisayar, cep telefonu, flash disk vb.) çalınması ve kaybolması gibi nedenlerle ortaya çıksa da elektronik posta ya da posta ile aktarılacak kişisel verilerin de dikkatli bir şekilde ve yeterli tedbirler alınarak gönderilmesi gerekmektedir. Ayrıca çalışanların şahsi elektronik cihazlarının, bilgi sistem ağına erişim sağlaması da güvenlik ihlali riskini arttırdığından bunlar için de mutlaka yeterli güvenlik tedbirleri alınmaktadır.

Kişisel veri güvenliğinin sağlanması için kişisel veri içeren kağıt ortamındaki evraklar, sunucular, yedekleme cihazları, CD, DVD ve USB gibi cihazların ek güvenlik önlemlerinin olduğu başka bir odaya alınması, kullanılmadığı zaman kilit altında tutulması, giriş çıkış kayıtlarının tutulması gibi fiziksel güvenliğin arttırılmasına ilişkin önlemler de alınmalıdır. Kişisel veri içeren cihazların kaybolması veya çalınması gibi durumlara karşı erişim kontrol yetkilendirmesi ve/veya şifreleme yöntemlerinin kullanılması kişisel veri güvenliğinin sağlanmasına yardımcı olacaktır. Bu kapsamda şifre anahtarı, sadece yetkili kişilerin erişebileceği ortamda

saklanmalı ve yetkisiz erişim önlenmelidir. Benzer şekilde, kişisel veri içeren kağıt ortamındaki evraklar da kilitli bir şekilde ve sadece yetkili kişilerin erişebileceği ortamlarda saklanmaktadır, söz konusu evraklara yetkisiz erişim önlenmektedir. Bunlarla birlikte şifreleme farklı farklı formlarda kullanılan ve bu formlara göre farklı şartlar sağlayan bir güvenlik sağlama aracıdır. Bu kapsamda, tam disk şifrelemesiyle cihazın tümü şifrelenebilir ya da cihazda bulunan bir dosya şifrelenmektedir. Bazı yazılımlar ise verilerde değişiklik yapılmasına izin vermemek için şifre koruması sunmakla birlikte bu yazılımlar kişisel verinin yetkisiz kişiler tarafından okunmasını durulur. Bu nedenle hangi şifreleme yöntemleri kullanılırsa kullanılsın kişisel verilerin tam olarak korunduğundan emin olunmaktadır. Tercih edilen şifreleme yönteminin asimetrik şifreleme yöntemi olması halinde, anahtar yönetimi süreçlerine önem verilmektedir.

5.4. Bilgi Teknoloji Sistemleri Tedariği, Geliştirme ve Bakımı

Veri sorumlusu tarafından yeni sistemlerin tedariği, geliştirilmesi veya mevcut sistemlerin iyileştirilmesi ile ilgili ihtiyaçlar belirlenirken güvenlik gereksinimleri göz önüne alınmaktadır. Uygulama sistemlerinin girdilerinin doğru ve uygun olduğuna dair kontroller yapılmaka, doğru girilmiş bilginin işlem sırasında oluşan hata sonucunda veya kasıtlı olarak bozulup bozulmadığını kontrol etmek için uygulamalara kontrol mekanizmaları yerleştirilmektedir. Uygulamalar, işlem sırasında oluşacak hataların veri bütünlüğünü bozma olasılığını asgari düzeye indirecek şekilde tasarlanmaktadır. Arızalandığı ya da bakım süresi geldiği için üretici, satıcı, servis gibi üçüncü kurumlara gönderilen cihazlar eğer kişisel veri içermekte ise bu cihazların bakım ve onarım işlemi için gönderilmesinden önce, kişisel verilerin güvenliğinin sağlanması için cihazlardaki veri saklama ortamının sökülerek saklanması, sadece arızalı parçaların gönderilmesi gibi işlemler yapılır. Bakım ve onarım gibi amaçlarla dışarıdan personel gelmişse kişisel verileri kopyalayarak kurum dışına çıkartmasının engellenmesi için gerekli önlemlerin alınmaktadır.

6. Kişisel Verilerin Yedeklenmesi

Kişisel verilerin herhangi bir sebeple zarar görmesi, yok olması, çalınması veya kaybolması gibi hallerde veri sorumlularının yedeklenen verileri kullanarak en kısa sürede faaliyete geçmesi gerekmektedir. Ayrıca kötü amaçlı yazılımlar da halihazırdaki verilere erişime engel olabilmektedir. Örneğin elektronik cihazlardaki kişisel verileri içeren dosyaları kilitleyen ve bunların açılabilmesi için veri sorumlusunu fidye ödemeye zorlayan kötü amaçlı yazılımlar olabilir. Bu tür kötü amaçlı yazılımlara karşı kişisel veri güvenliğini sağlamak için veri yedekleme stratejilerinin geliştirilmektedir. Öte yandan, yedeklenen kişisel veriler sadece sistem yöneticisi tarafından erişilebilir olup, veri seti yedekleri mutlaka ağ dışında tutulmaktadır. Bu sayede veri seti yedekleri üzerinde kötü amaçlı yazılım kullanımı veya verilerin silinmesi ve yok olması durumlarıyla karşı karşıya kalınması önlenmektedir. Bu nedenle tüm yedeklerin fiziksel güvenliğinin de sağlandığından emin olunmak üzere çalışmalar yapılmaktadır.

7. Veri aktarımları

EKİP MÜHENDİSLİK, hakkınızda topladığı kişisel bilgileri, internet servisi sağlayıcılarının, hosting şirketlerinin, e-mail tedarikçilerinin, domain sağlayıcılarının hizmetlerinin kullanılması nedeniyle, bu bilgilerin toplanıldığı ülkeden başka ülkelere aktarabilir. Bu ülkelerde uygulanan verilerin korunmasına ilişkin mevzuatlar, Türkiye'de uygulanan mevzuattan farklı olabilir.
Verileriniz, başka ülkelere aktarma sırasında işbu Gizlilik Politikasında açıklandığı üzere yürürlükteki yasaya uygun olarak korunacaktır.

8. Çocukların online faaliyetlerini koruma

EKİP MÜHENDİSLİK tarafından hiçbir durumda kasten çocuklardan kişisel bilgileri istenmemektedir. Eğer kişisel bilgileri alınan bir kişinin 13 yaşının altında olduğu öğrenilirse durumu derhal ebeveynlerine bildirmeye çalışmak için bu bilgi kullanılır. Bu kural Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), kapsamında 16 yaş için uygulanır.

9. Yeni süreçleri gizlilik kurallarına uygun tasarlama

EKİP MÜHENDİSLİK yeni sistemler geliştirirken gizlilik için en uygun teknolojik ve organizasyonel tedbirleri alır ve amaca uygun olarak kişisel verilerin işlenmesi için gerekli geliştirmeleri yapılır. (Privacy by design)