Grup ENERGO-PRO

ÇALIŞAN (DAHİLİ) VERİLERİ KORUMA POLİTİKASI

2021

ÇALIŞAN (DAHİLİ) VERİLERİ KORUMA POLİTİKASI

1. Giriş

Ana faaliyet alanımız hidroelektrik sektörüdür. Orta ve Doğu Avrupa'da, Karadeniz'de ve Kafkaslarda hidroelektrik santralleri işletmekteyiz. Aynı zamanda, elektrik dağıtımı ve enerji ticaretiyle iştigal etmekte ve Bulgaristan ve Gürcistan'da 2,3 milyonu aşkın şebeke müşterisine sahip büyük ölçekli dağıtım şebekeleri işletmekteyiz.

Şirketimiz 1994 yılında, Çekya'nın Svitavy ilçesinde kurulmuş olup ekonomik geçiş dönemi sırasında Orta ve Doğu Avrupa'da hidroelektrik santrali modernizasyonuna ve rehabilitasyonuna iştirak etmiştir. Enerji santrallerimizin toplam kurulu kapasitesi 1.243 MW düzeyinde olup yıllık güç üretimiyse 3,8 TWh düzeyini aşmaktadır.

Dünya çapında 60'tan fazla ülkeye proje teslim etmiş olan Sloven su türbinleri üreticisi Litostroj Power d.o.o. grubumuzun bir parçasıdır. Onun Çek Cumhuriyeti siciline kayıtlı olan yan kuruluşu Litostroj Engineering a.s. şirketi (eski adıyla ČKD Blansko Engineering, a.s.), araştırma, tasarım ve mühendislik işlerine odaklanmaktadır. Litostroj Group aynı zamanda pompaj depolamalı hidroelektrik santralleri ve pompaj istasyonları dahil olmak üzere hidroelektrik santrallerine donanım tedarik etmektedir.

2. Bu ne hakkındadır

Bu, ENERGO-PRO Group'a ait veri koruma politikasıdır[1] ("**biz**", "**bizi**", "**bizim**"). Bunun ENERGO-PRO için ya da onunla birlikte çalışan tüm çalışanlar, yükleniciler, geçici işçiler, temsilciler ve danışmanlar (**"personel"** ya da **"siz"**) tarafından takip edilmesi gerekir.

Çalışanlarımız hakkındaki kişisel verileri elimizde tutuyoruz.

Bu politikada kişisel verileri nasıl korumayı amaçladığımız ve personelin, çalışmaları sırasında erişim sahibi oldukları kişisel verilerin kullanımına ilişkin kuralları anlamalarını nasıl sağladığımız ortaya konulmaktadır. Bu politika özellikle, herhangi bir önemli yeni veri işleme faaliyeti başlamadan önce ilgili uyum adımlarının yerine getirildiğinden emin olmak üzere personelin Veri Koruma Görevlisine (DPO) danışmasının sağlamasını şart koşmaktadır.

Bu politika, tüm iş alanları genelinde genel uygulama niteliğinde bilgi ve rehberlik sağlamaktadır. Bu neden önemlidir?

Kişisel verileri sorumluluk ve yasalara uygunluk çerçevesinde kullanmadığımız takdirde bu durum insanların işimize duydukları güveni olumsuz etkileyebilir. Ayrıca, hassas ticari bilgilerimiz gizli niteliktedir ve uygun şekilde korunmaları gerekir, aksi takdirde bu durum rekabet avantajımızı kaybetmemiz, itibarımızın zarar görmesi ya da yasal yükümlülüklere maruz kalmamızla sonuçlanabilir.

Daha da önemlisi, veri koruma yasalarına riayet etmediğimiz takdirde ağır düzenleyici cezalarla da çarptırılabiliriz (20 milyon Euro'ya kadar ve yıllık küresel cironun %4'üne kadar).

3. Tanımlar

Aşağıdaki ifadeleri anlamanız önemlidir:

"Veri koruma kanunları", GDPR ve çalıştığınız ülkede ya da bilgilerini kullandığınız kişiler açısından geçerli olan her türlü yerel kanunlar da dahil olmak üzere kişisel verilerin gizliliğini, kullanımını ve korunmasını düzenleyen yasalar kanunlar anlamına gelmektedir.

"GDPR", 25 Mayıs 2018 tarihinden itibaren Avrupa Birliği (**"AB"**) genelinde geçerli olan ve AB'de kurulmuş kuruluşları ve ayrıca AB'deki bireylerin kişisel verilerini Avrupa Birliği'nde

[1] Gruba; ENERGO-PRO a.s. şirketinin tek ve doğrudan hissedarı olan DK Holding Investments, s.r.o. ve onun tüm dolaysız ve dolaylı yan kuruluşları dahildir.

kullanan AB dışında yer alan kuruluşları etkileyen Genel Veri Koruma Yönetmeliği anlamına gelmektedir.

"Kişisel veriler", kimliği belirli ya da belirlenebilir durumda olan gerçek bir kişiye (yani, kimliği doğrudan ya da dolaylı olarak, özellikle bir tanımlayıcıya ya da o kişinin fiziksel, fizyolojik, genetik, zihinsel, ekonomik, kültürel ya da sosyal kimliğiyle belirlenebilen) yönelik her türlü bilgi anlamına gelmektedir. Tanımlayıcılar arasında adlar, kimlik numaraları, konum verileri ve çevrimiçi tanımlayıcılar gibi öğeler yer almaktadır.

Kişisel verilerini topladığımız kişi türlerine ilişkin örnekler: mevcut ve eski çalışanlar, acente, sözleşmeli ve diğer personel, müşteriler, tedarikçiler ve pazarlama bağlantıları.

Topladığımız kişisel veri türlerine ilişkin örnekler: bireylerin irtibat bilgileri, eğitim geçmişi, mali ayrıntılar ve ödeme ayrıntıları, sertifika ve diploma bilgileri, eğitim ve beceriler, medeni durum, uyruk, iş unvanı, sağlık verileri, biyometrik veriler ve özgeçmiş.

Tamamen anonimleştirilmiş veriler (yani bir bireyin kimliğinin tespit edilemediği veriler) ve vefat etmiş kişilerle ilgili bilgiler genellikle kişisel veri olarak kabul edilmez.

"Özel kategorideki kişisel veriler" ırk ya da etnik köken, siyasi görüş, dini ya da felsefi inançlar ya da sendika üyeliğini ortaya çıkaran kişisel veriler; genetik verilerin, biyometrik verilerin gerçek bir kişinin kimliğinin benzersiz şekilde belirlenmesi amacıyla işlenmesi; sağlıkla ilgili veriler ya da gerçek bir kişinin cinsel hayatı ya da cinsel yönelimi ile ilgili veriler anlamına gelmektedir

Özel kategorideki veriler (bazen eski adıyla "hassas kişisel veriler" olarak anılır) ilgili olduğu kişiye zarar verme potansiyeli taşıdığından özel bir koruma gerektirmekte olup bundan dolayı bu politikaya göre sıkı bir şekilde kontrol edilmelidir.

Sağlık verileri muhtemelen bu kategoride karşılaşacağınız en tipik verilerdir (hem fiziksel hem de zihinsel sağlığı kapsar) ve sağlık durumunuz hakkında bilgi sağlayan her unsuru kapsar.

"Veri işleme" verilerin toplanması, kaydedilmesi, düzenlenmesi, yapılandırılması, depolanması, uyarlanması ya da değiştirilmesi, geri alınması, danışılması, kullanılması, iletim, yayma ya da başka bir şekilde kullanıma sunma, uyarlama ya da birleştirme, kısıtlama, silme ya da imha yoluyla açıklanması gibi otomatik araçlarla olsun ya da olmasın kişisel veriler ya da kişisel veri dizileri üzerinde gerçekleştirilen her bir faaliyet ya da faaliyet dizisi anlamına gelmektedir. Kişisel verilerle yaptığınız neredeyse her şey veri işlemedir.

"Veri İhlalleri" iletilen, saklanan ya da başka bir şekilde işlenen kişisel verilerin kazara ya da yasadışı imhasına, kaybına, tahrifatına, yetkisiz olarak açıklanmasına ya da erişilmesine yol açan her türlü güvenlik ihlali anlamına gelmektedir.

4. Kapsam

Bu politika tüm personel için geçerlidir. Bu politikayı bilmeniz ve şartlarına riayet etmeniz gerekmektedir.

Bu politikayı zaman zaman ek politikalar ve yönergelerle destekleyebilir ya da tadil edebiliriz ve bu durumda önemli değişiklikler hakkında sizi bilgilendiririz.

5. Bu politikadan kim sorumludur?

Veri koruma görevlisi bu politikanın genel sorumluluğunu üstlenmektedir. Tüm personelin bu politikaya riayet etmesini sağlamakla sorumludur.

Ancak, verilerin korunmasına uyumumun doğru olarak anlaşılması herkesin menfaatine olup ve tüm personelin sorumluluğundadır. Bir veri koruma sorunu (ya da potansiyel bir sorun) tespit ettiğiniz takdirde bunu bildiriniz ve hızlı bir şekilde ele alınız ve ihtiyacınız olan durumlarda daima destek isteyiniz.

6. Prosedürlerimiz

Yasal, adil ve şeffaf işleme

Kişisel verileri bireylerin haklarını ihlal etmeksizin hukuka uygun, adil ve şeffaf bir şekilde işlememiz gerekir. Bu, genellikle, kişisel verileri aşağıdaki durumlar haricinde işlememiz gerektiği anlamına gelir:

- işlemenin:
  - (a) bir kişiyle yapmış olduğumuz bir sözleşmeyi (bir iş sözleşmesi dahil) ifa etmek ya da sahip olduğumuz yasal yükümlülükleri yerine getirmek için gerekli olması; ya da
  - (b) meşru menfaatlerimiz açısından başka bir şekilde gerekli olması ve bireyin veri koruma hakları tarafından geçersiz kılınmamış olması; ya da
- bilgilerini işlediğimiz kişinin buna rıza göstermiş olması.

İznin özgür iradeyle verilmiş olması, belirli, bilgilendirilmiş ve net olması ve bireyin kişisel verilerinin işlenmesini kabul ettiğini gösteren bir beyan ya da açık bir olumlu eylem yoluyla verilmiş olması gerekir. İzinlerin kayıtlarını tutmanız gerekir. Bir kişinin bilgilerini işlememize ilişkin onayını geri çekmesi durumunda bu bilgileri işlemeyi durdurmamız gerekir.

Mümkün olan her durumda yukarıdaki ilk madde başlığında yer alan alternatif gerekçelerden birine yönelik olarak (özellikle istihdamla ilgili bilgiler için) işlemeye izin verilmesini sağlamaya çalışmalıyız. Bu hüküm çoğu durumda rutin iş verileri işleme faaliyetleri açısından geçerli olacaktır.

Özel kategorideki kişisel veriler

Özel kategorideki kişisel verileri işlediğimiz çoğu durumda, istisnai koşullar geçerli olmadığı ya da kanunen bunu yapmamız gerekmediği sürece (örn. iş yerinde sağlık ve güvenliği sağlamaya yönelik yasal yükümlülüklere uymak için ya da birisi ciddi şekilde yaralandıysa ve rıza gösteremeyecek durumdaysa) veri sahibinin açık şekilde verilmiş rızasına sahip olmamız gerekir.

Herhangi bir rıza ilgili verilerin ne olduğunu, neden işlendiğini ve kime açıklanacağını açık bir şekilde belirtmelidir. Bireyin ideal olarak sözcüklerle ve (mümkünse) imza atılmış ve tarihi belirtilmiş bir beyanla yanıt vermesi gerekecektir. Belirli sağlık amaçları için bir rıza formu kullanmaktayız. (Bkz. Ek 1.)

Belirtilen amaçlar için işleme

Kişisel verileri toplamak için "sonradan belirlenecek gerekçeler" yeterli değildir. Kişisel verilerin yalnızca kişiye anlattığınız belirli amaçlara yönelik olarak toplandığından emin olmanız gerekir. Bu verileri daha sonra tamamen farklı bir şey için kullanma kararı alamazsınız (birçok durumda geri dönüp bu verileri böylesi farklı bir amaç için kullanmak üzere izin istemeniz gerekir).

Verileri azaltma ve doğruluk

İşlediğimiz tüm kişisel verilerin doğru, uygun, alakalı ve elde edilme amacına kıyasla aşırı nitelikte olmamasını sağlayacağız.

Elimizde bulunan kişisel verilerin doğru kalmasını sağlamak için periyodik kontroller yapmanız ve gerektiğinde bunları güncellememiz gerekir. Bireyler kendileri ile ilgili yanlış kişisel verileri düzeltmemizi isteyebilirler. Bilgilerin yanlış olduğuna inanıyorsanız, bilgilerin doğruluğunun tartışmalı olduğunu kaydederek veri koruma görevlisine bildirimde bulunmanız gerekir. Yanlış, yanıltıcı, hatalı ya da güncel olmayan verilerin güncellenmesi ya da muhtemelen imha edilmesi gerekebilir – bu durumdan emin değilseniz lütfen veri koruma görevlisi ile görüşünüz.

Kişisel verileri toplamak için formlar ya da süreçler oluştururken bunların daha fazlasını değil ancak gerektiği kadar asgari veriyi yakalamasını sağlamanız gerekir - toplanmakta olduğu ya da toplanmış olduğu amaç için gerekli olmayan herhangi bir verinin en başından toplanmaması gerekir. İlgili kişi bunu kabul etmediği ya da makul bir şekilde bunu beklemediği sürece tek bir amaç için elde edilen kişisel verileri bağlantılı olmayan herhangi bir amaç için işlemeyeceğiz.

7. Veri güvenliği

Kişisel verilerin kazara ya da yasadışı imhaya, kayba, tahrifata, yetkisiz olarak açıklanmaya ya da erişilmeye karşı güvenlik altında tutulması gerekir. Bu, güvenlik yönergelerimize ve politikalarımıza riayet edilmesi anlamına gelir.

Verilerin güvende kalmasını sağlamak için uygun teknik ve organizasyonel önlemleri uygulama yükümlülüğümüz bulunmaktadır. Örnek vermek gerekirse duruma bağlı olarak aşağıdakiler uygun olabilir:

- verilere erişim haklarınının yalnızca onu bilmesi gereken belirli yetkili kişilerle sınırlandırılması (erişim kontrolleri);
- kimliği gizlenmiş (örn. anonimleştirilmiş ya da anahtar kodlu) verilerin kullanılması;
- kilitlenebilir masaların ve dolapların güvenli tutulması. Kişisel verileri (ve gizli bilgileri) içeren masalar ve dolapların kilitli tutulması;
- kişisel verilerin güvenli bir şekilde elden çıkarılması. Basılı belgeler kıyılarak imha edilmelidir. Disketler, CD-ROM'lar, USB'ler artık gerekli olmadıklarında fiziksel olarak imha edilmelidir; ya da
- donanımın güvenli şekilde kullanılması. Ziyaretçiler gibi üçüncü şahısların kişisel verileri şirket monitörleri üzerinde görememesinin sağlanması. Kullanıcısının başında bulunmadığı bilgisayarlarda oturumun kapalı olması.

Uygulamalar ve bulut tabanlı servisler konusunda özellikle dikkatli olmamız gerekmektedir. Verileri bir uygulamaya koyup onu veri koruma görevlisinin onayını almadan buluta yüklemeyiniz.

Ayrıca, kişisel verilere erişmek için kullandığınız cihazların daima zaman şifreli olduğundan ve kişisel verileri başkalarıyla paylaşırken uygun korumaların uygulandığından emin olunuz.

Veri güvenliği işletmemiz için hem bir önceliktir hem de süregelen bir mücadeledir. Kişisel verileri işlemek için kullandığımız teknik ve organizasyonel güvenlik tedbirlerinin etkinliğini düzenli olarak test etmemiz, incelememiz ve değerlendirmemiz gerekir.

Verilerin saklanması

Kişisel verileri gerekenden daha uzun süre saklamamalıyız. Gerekli olan süre kişisel verilerin elde edilme gerekçeleri dikkate alınarak her bir durumun koşullarına bağlı olacak olup Veri Saklama İlkelerimize uygun bir şekilde belirlenmelidir. (Bkz. Ek 2.)

Kişisel verileri imha ya da silme işlemlerinin güvenli bir şekilde yapılması gerekir.

Örnek vermek gerekirse, bunların analitik ya da istatistiksel amaçlar için yararlı olduğu durumlarda, bilgilerin kimliğini belirli bireylerin bu bilgilerden tanımlanamayacağı şekilde gizlemek mümkünse bunları daha uzun bir süre boyunca elimizde tutabiliriz.

Kişisel verileriniz

Sizin hakkınızda tuttuğumuz kişisel verilerin doğru ve gerektiğinde güncel olduğundan emin olmak için makul adımları atmanız gerekir, örn. kişisel durumunuzda değişiklik olursa kayıtlarınızı güncelleyebilmeleri için lütfen İK Departmanını bilgilendiriniz.

8. Verilerin uluslararası olarak aktarılması

Kişisel verilerin uluslararası aktarımlarına dair kısıtlamalar bulunmaktadır. Uluslararası bir veri aktarımı, yalnızca, kişisel verileri AEA dışındaki bir alıcıya gönderdiğinizde değil, aynı zamanda kişisel verilere AEA dışından erişim ya da görüntüleme yapıldığında da gerçekleşebilir.

Kişisel verileri, ilk olarak veri koruma sorumlusuna danışmaksızın AEA dışına (AB, İzlanda, Lihtenştayn ve Norveç dahil) aktarmamanız gerekir. Genel olarak, kişisel verilerin AEA dışına yasal olarak aktarılabilmesi için belirli sözleşmelerin ya da alternatif aktarım mekanizmalarının uygulanmakta olması gerekir.

Merkezi AEA dışında bulunan ya da AEA dışında bulunan altyükleniciler kullanan tedarikçilerle çalışırken onların sağladıkları hizmetlerin belirli yönleri açısından özellikle dikkatli olmanız gerekir. Bulut tabanlı hizmetleri kullanırken veriler için hosting hizmeti sağlanan konumları kontrol etmeniz ve uluslararası veri aktarımlarına ilişkin gereksinimlere uyulduğundan emin olmanız gerekir.

9. Veri sahibinin erişim talepleri

GDPR kapsamında, bireyler (belirli istisnalara tabi olarak) kendileri hakkında tutulan bilgilerin bir kopyasına erişim talep etme hakkına sahiptir. Bu, sizin ve diğer çalışanların onların kayıtlarına eklediğiniz herhangi bir görüşü de içerebilir. Bunlar bazen "SAR" ("veri sahibi erişim talepleri" anlamına gelir) olarak anılmaktadır.

Bireyler ayrıca düzeltme, silme, kısıtlama, veri taşınabilirliği talep etme, işlemeye itiraz etme ve otomatik karar verme ve profil çıkarmaya ilişkin diğer haklara da sahiptirler.

Böylesi çeşitli haklar veri sahibi talepleri (DSR) olarak adlandırılır. Bir veri sahibi talebi aldığınızda lütfen bu talebi derhal veri güvenlik sorumlusuna iletiniz ve Ek 3'te yer alan veri sahibi talebi prosedürümüzü izleyiniz. Bu taleplere uyabilmemiz için bize yardım etmenizi isteyebiliriz, ancak, veri güvenliği sorumlusu ile iletişime geçmeden talebi onaylamak için dahi yanıt vermemelisiniz.

Veri sahibi taleplerini yanıtlamak için ücret talep edememekteyiz, ancak, bir talep açıkça asılsız ya da aşırı olduğunda takdirde ve özellikle de mükerrer nitelikteyse idari maliyetlerimize karşılık ücret talep edebiliriz.

Hiçbir veri sahibi talebi mutlak değildir - bir kişinin hak sahibi olduğu bilgilere ya da veri koruma kanunları uyarınca bir kuruluşun bir talebe yanıt olarak ne yapmasını şart koşabileceğine ilişkin istisnalar ve kısıtlamalar bulunmaktadır.

Bir veri sahibi talebi yapmak istiyorsanız nasıl hareket etmelisiniz?

Elimizde bulundurduğumuz size ilişkin bilgileri düzeltmek ya da talep etmek ya da yukarıda belirtilen diğer haklarınızdan herhangi birinden yararlanmak istiyorsanız lütfen veri koruma görevlisi ile iletişime geçiniz.

10. Veri ihlallerinin bildirilmesi

Gerçek ya da potansiyel veri koruma uyumluluğu hatalarını bildirme yükümlülüğü tüm personele aittir. Bu bizim aşağıdakileri yapmamızı mümkün kılar:

- sorunu soruşturmak ve gerekiyorsa düzeltici adımları atmak; ve,
- bunu yapmanın makul olduğu durumlarda ihlali düzenleyici makamlara ya da polise bildirmek.

Bir veri ihlalini bildirmekte gecikmeyiniz – ihlali kontrol altına almak için zaman kritik öneme sahip olacaktır ve ayrıca kişisel veri ihlallerini ilgili düzenleyicilere (genellikle 72 saat içinde) bildirme yükümlülüğümüz bulunmaktadır. Bu gerçekten çok önemlidir.

Önleme en güçlü savunma biçimidir. Güvenlik riski oluşturabilecek herhangi bir şey gördüğünüz takdirde bunu derhal bölüm yöneticinize bildiriniz.

11. Eğitim

Tüm personel bu politika hakkında eğitim görecektir. İşe yeni başlayanlar oryantasyon sürecinin bir parçası olarak eğitim göreceklerdir. Kanunda ya da politikamızda ve prosedürümüzde önemli bir değişiklik olması halinde daha ileri şekilde eğitim sağlanacaktır.

Eğitim online olarak verilmektedir.

Aşağıdakileri kapsayacaktır:

- verilerin korunmasına ilişkin kanun; ve,
- veri koruma ve alakalı politikalarımız ve prosedürlerimiz.

Eğitimin tamamlanması mecburidir.

Veri koruma görevlisi eğitim ihtiyaçlarını sürekli olarak gözlemleyecek olsa da ilgili kanunun ya da bu politikanın ya da prosedürlerin herhangi bir unsuru hakkında daha fazla eğitime ihtiyaç duyduğunuzu düşünüyorsanız lütfen veri koruma görevlisi ile iletişime geçiniz.

12. İzleme

Bu politikaya herkesin uyması gerekmektedir. Veri koruma görevlisi bu hususa riayet edilmesini sağlamak için bu politikayı düzenli olarak izleme konusunda genel sorumluluğa sahiptir.

13. Bu politikaya riayet edilmemesi

Bu politikaya riayet edilmesini oldukça ciddiye alıyoruz.

Riayet edilmemesi hem sizi hem de şirketi riske sokmaktadır.

Bu politikanın önemi herhangi bir gerekliliğe uyulmamasının prosedürlerimiz kapsamında işten çıkarılmaya varan disiplin işlemlerine yol açabileceği anlamına gelmektedir.

Bu politikayla ilgili herhangi bir sorunuz ya da endişeniz varsa çekinmeden veri koruma görevlisi ile iletişime geçiniz.

EK 1

ÖZEL KATEGORİDEKİ KİŞİSEL VERİLERİN İŞLENMESİ RIZA FORMU

BEYAN

Aşağıda imzası bulunan ben

_____

(Adı, göbek adı ve soyadı)

Kişisel Tanımlama Numarası (ya da eşdeğeri) : _____, unvanım:

0 Şirket çalışanı

_____

0 Şirket çalışanının eşi, hayat arkadaşı, 18 yaşından büyük çocukları

_____

0 Yetkili temsilcisi olduğu

_____

0 Diğer / lütfen açıklayınız /:

_____

AŞAĞIDAKİ HUSUSLARI BEYAN EDERİM:

devlet tarafından ve/ya da herhangi bir zorunlu sağlık sigortası kapsamında ödemesi yapılmayan bir hastalığın tedavisiyle bağlantılı olarak ya da buna yönelik amaçlarla [maddi destek gibi amaçlarla) sağladığım kişisel verilerin (sağlık verilerim dahil) ENERGO-PRO tarafından aşağıdaki belgelerde işlenebileceğini ve saklanabileceğini kabul ederim:

[0 Mali destek başvurusu [herhangi bir geçerli sağlık fonu];]
[0 Başvuruda açıklanan tıbbi belgeler;]
[0 Diğer / lütfen açıklayınız /:]

_____

aşağıdakilerin gereklilikleri uyarınca:

• Kişisel verilerin işlenmesine yönelik olarak bireylerin korunmasına ve bu tür verilerin serbest dolaşımına ilişkin 27 Nisan 2016 tarihli Avrupa Parlamentosu ve Konseyi'nin (AB) 2016/679 sayılı Yönetmeliği ((AB) 2016/679 sayılı Yönetmelik); ve
• Ulusal Veri Koruma Kanunları ve Yönetmelikleri,

Aşağıdaki hususlar bilgim dahilindedir:
- kişisel verilerimin (sağlık verilerim dahil) işlenmesinin amacı ve araçları;
- kişisel verilerin sağlanmasının gönüllüğe dayalı niteliği;

- toplanan verilere ilişkin erişim ve düzeltme ya da silme hakkı ve kişisel verilerin işlenmesini kısıtlama hakkı;
- işlemeye itiraz etme hakkı ve ayrıca kişisel verilerimin üçüncü bir şahsa - kişisel veri toplayıcı - aktarılmasını talep etme hakkı;
- kişisel verilerimin işlenmesiyle bağlantılı olarak Ulusal Veri Koruma Kurumuna [web sitesi bağlantısı ekleyiniz] itirazda bulunma hakkı;
- ENERGO-PRO group şirketlerinin veri koruma politikası;
- veri koruma görevlisinin iletişim bilgileri: [veri koruma görevlisi'nun e-posta adresini ekleyiniz]; ve
- ENERGO-PRO'nun kişisel verilerimi (sağlık verilerim dahil) dünya çapında aktarmasının gerekebileceği ve kişisel verilerimi ENERGO-PRO adına işlemek için üçüncü şahısları kullanabileceği.

_____

(Yukarıda açıklanan şekildeki işleme konusunda bilgilendirildim ve bunu kabul ediyorum)

Rızamı özgür irademle vermekteyim ve herhangi bir zamanda rızamı kısmen ya da tamamen vermeyi reddetme ve halihazırda verilmiş olan rızamı geri çekme hakkına sahip olduğum konusunda bilgilendirilmiş bulunmaktayım. Rızamı geri çekiyor olmak bunu geri çekmeden önceki bir rızaya dayalı olarak yapılmış işlemenin yasallığını etkilemez.

[Reddetmem durumunda (tam/kısmi) yukarıda belirtilen başvurunun değerlendirilmesine devam edilmeyebileceği konusunda bilgilendirildim.]

Tarih: _____ Beyan sahibi: _____
(imza)

Yer: _____

* el yazısıyla doldurulacaktır

EK 2

VERİ SAKLAMA YÖNERGELERİ

Kişisel verileriniz yalnızca, öngörülen amaçlara ulaşmak için gerekli olan süre boyunca saklanır.

İş ilişkilerinin ifası konusunda yalnızca kanunun şart koştuğu kişisel veriler iş ve sosyal güvenlik mevzuatının öngördüğü şartlar dahilinde işlenecek ve saklanacaktır.

Veri saklama ile ilgili yasal zorunlulukların mevcut olmaması halinde veriler 5 yıllık bir süreye kadar saklanabilir.

EK 3

VERİ SAHİBİNİN ERİŞİM TALEPLERİ

Bize daha önce vermiş olduğunuz Kişisel Verilere dair erişim, düzeltme, silme, kısıtlama ya da işlenmesine itirazda bulunmak istediğiniz ya da Kişisel Verilerinizin elektronik bir kopyasını başka bir şirkete iletmek amacıyla (veri taşınabilirliği hakkının size yürürlükteki yasa tarafından sağlandığı ölçüde) almak için bir talepte bulunmak istediğiniz takdirde bizimle e-posta yoluyla iletişime geçebilirsiniz ([veri koruma görevlisinin e-posta adresini ekleyiniz]). Talebinizi yürürlükteki kanun çerçevesinde yanıtlayacağız.

Hangi talebi yapıyor olursanız olun ilgili talep söz konusu verilerin ayrıntılı ve doğru bir açıklamasını içermelidir. Kimliğinizle ilgili makul şüpheler söz konusu olduğu takdirde kimliğinizi doğrulamamıza yardımcı olacak bir belgenin kopyasını sunmanız talep edilebilir. Bu, nüfus cüzdanınız ya da pasaportunuz gibi herhangi bir uygun belge olabilir. Başka herhangi bir belge sunmanız durumunda kimliğinizi tespit edebilmek için adınız ve adresiniz gibi kişisel bilgilerin açık şekilde görülmesi gerekirken, fotoğrafınız ya da herhangi bir kişisel özelliğiniz gibi diğer veriler karalanmış olabilir.

Nüfus cüzdanı belgenizde yer alan bilgileri kullanımımız kesinlikle sınırlandırılmıştır: veriler yalnızca kimliğinizi doğrulamak için kullanılacak olup bu amaç için gerekli olandan daha uzun bir süre saklanmayacaktır.
Lütfen hangi Kişisel Verilerin değiştirilmesini istediğinizi, Kişisel Verilerinizin veri tabanımızdan kaldırılmasını isteyip istemediğinizi ya da Kişisel Verilerinizi başka şekilde kullanmamız açısından ne tür sınırlamalar getirmek istediğinizi talebinizin niteliğine bağlı olarak açık şekilde belirtiniz. Güvenliğiniz için yalnızca hesabınızla ilişkili Kişisel Verilere, e-posta adresinize ya da diğer hesap bilgilerinize ya da talebinizi bize göndermek için kullanmış olduğunuz size ilişkin diğer belirli bilgilere ilişkin talepleri işleme koyabiliriz ve talebinizi işleme koymadan önce kimliğinizi doğrulamaya gerek duyabiliriz.

Belirli bilgileri kayıt tutma amacıyla saklamamız gerekebileceğini lütfen unutmayınız. Veritabanlarımızda ve diğer kayıtlarımızda kalacak ve kaldırılmayacak artık bilgiler söz konusu olabilir.

Talebinizi/taleplerinizi makul olarak uygulanabilir olan en kısa sürede yerine getireceğiz.