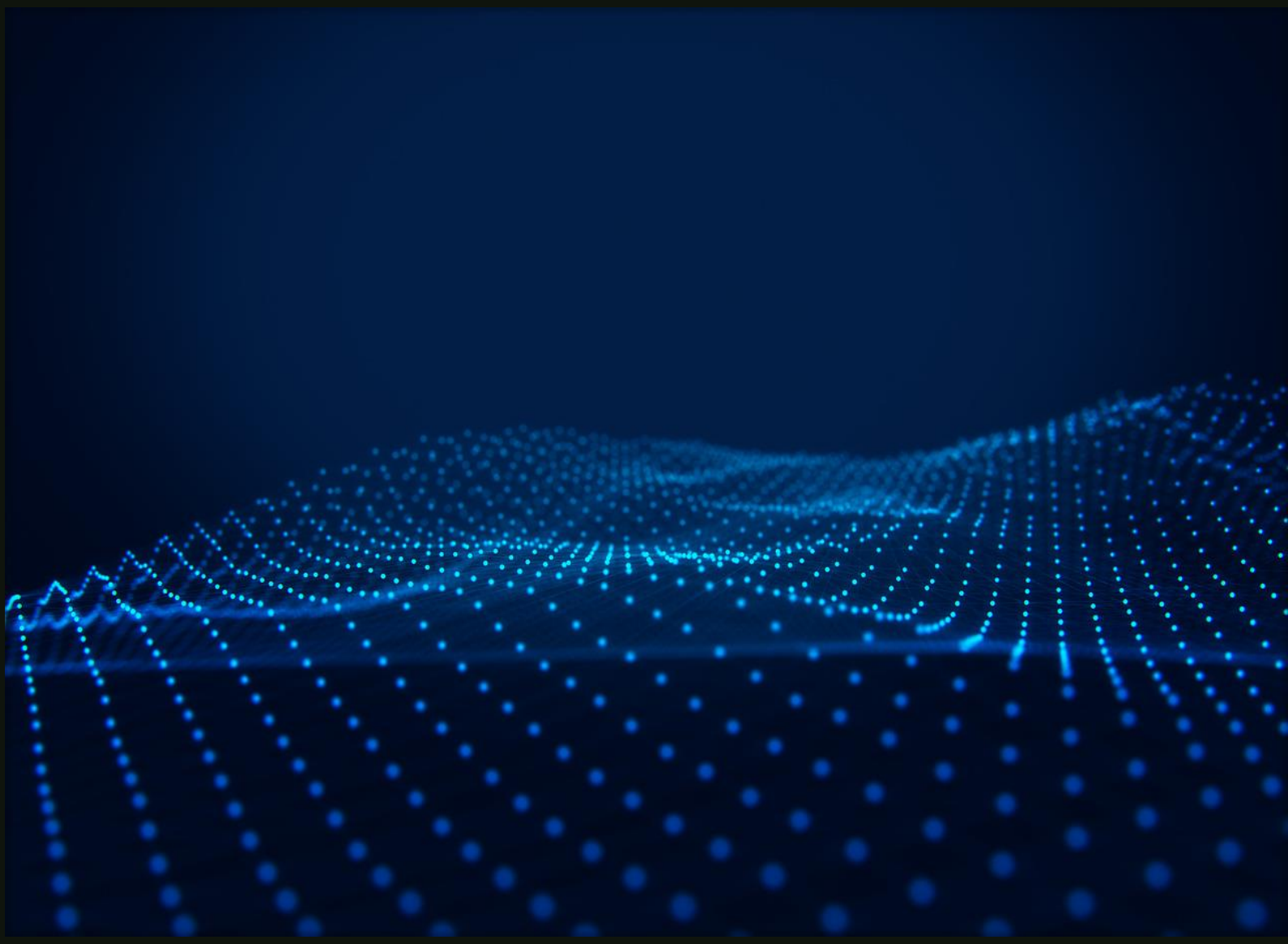

AB Veri Koruma Yönetmeliği

Mercedes-Benz Group

Mercedes-Benz

İçindekiler

1 Yönetmeliğin hedefi 3

2 Uygulama alanı 3

3 Mercedes-Benz Group içerisinde yasal bağlayıcılık 4

4 Yasal gereksinimlere istinaden 4

5 Kişisel verilerin işlenmesi ile ilgili genel temel kurallar 5

5.1 Yasallık 5

5.2 Müşteri ve ortak verilerinin yasal dayanağı 5

5.2.1 Sözleşmesel bir ilişki için veri işleme 5

5.2.2 Reklam amaçlı veri işleme 5

5.2.3 Veri işleme için muvafakat 6

5.2.4 Yasal izinler veya zorunluluk sebebiyle veri işleme 6

5.2.5 Meşru menfaatler sebebiyle veri işleme 6

5.3 Çalışan verileri için yasal dayanak 7

5.3.1 İş ilişkileri ile ilgili verilerin işlenmesi 7

5.3.2 Yasal izinler veya zorunluluk sebebiyle veri işleme 7

5.3.3 Verilerin işlenmesi için toplu anlaşma 7

5.3.4 Veri işleme için muvafakat 7

5.3.5 Meşru menfaatler sebebiyle veri işleme 8

5.4 Özellikle korunması gereken verilerin işlenmesi 8

5.5 Otomatikleştirilmiş münferit durum kararları (varsa Profiling dahil) 8

5.6 Bilgi verme yükümlülüğü/şeffaflık 9

5.7 Amaca uygunluk 9

5.8 Verilerin minimizasyonu 9

5.9 Verilerin doğruluğu 9

5.10 Privacy by Design & Privacy by Default 9

5.11 Silme ve anonimleştirme 10

5.12 Verilerin işlenmesinde güvenlik 10

5.13 (Diğer)Aktarımlar 11

6 Veri koruma sonuçlarının değerlendirilmesi 11

7 Veri işleme yöntemlerinin dokümantasyonu 11

8 İş emri üzerine işleme 11

8.1 Genel hususlar 11
8.2 Görevlendiren için düzenlemeler 12
8.3 Görevlendirilenler ile ilgili grup içerisindeki düzenlemeler 12
9 Ortak sorumluluk 13
10 İlgili kişiler için uygulanabilir haklar 13
10.1 İlgili kişinin hakları 14
10.2 Şikayet yöntemi 15
11 Sorumluluk ve yetkili mahkeme 15
11.1 Sorumluluk düzenlemeleri 15
11.2 Yetkili mahkeme 15
12 Veri koruma vakalarının bildirilmesi 16
13 Veri koruma organizasyonu ve yaptırımlar 16
13.1 Sorumluluk 16
13.2 Farkındalık oluşturma ve eğitim 17
13.3 Organizasyon 17
13.4 Yaptırımlar 18
13.5 Denetim ve kontroller 18
14 Yönetmelik değişiklikleri ve makamlarla iş birliği 18
14.1 Değişiklik durumunda sorumluluklar 18
14.2 Makamlarla iş birliği 19
15 Kişisel verilerin AB/AEA'dan üçüncü bir ülkeye aktarılması 19
15.1 Verilerin Mercedes-Benz Group dışına aktarılması 19
15.2 Verilerin Mercedes-Benz Group içine aktarılması 20
16 Üçüncü ülke düzenlemelerinin denetimi ve raporlanması 20

1 Yönetmeliğin hedefi

Mercedes-Benz Group, veri koruma haklarının korunmasını sosyal sorumluluğunun bir parçası olarak görmektedir.

Avrupa Birliği gibi bazı ülkelerde ve bölgelerde, kanun koyucu gerçek kişilere ait verilerin ("kişisel veriler") korunması için standartlar belirlemiştir. Buna bu verilerin, sadece varış ülkesinde alıcı tarafında uygun bir veri koruma seviyesi mevcut olduğunda başka ülkelere aktarılabileceği gerekliliği de dahildir.

Bu AB veri koruma yönetmeliği, aşağıdakiler için grup içerisinde tutarlı ve uygun veri koruma standartlarını belirlemektedir:

- (a) AB/ Avrupa Ekonomik Bölgesi (AEB) gibi bölgelerde (bundan sonra tutarlı olması açısından "**AB/ AEB**" olarak adlandırılacaktır) kişisel verilerin işlenmesi ve
- (b) kişisel verilerin AB/AEB dışındaki grup şirketlerine aktarılması (verilerin ilgili ülkelerde işlenmesi dahil).

Bu amaç doğrultusunda bu yönetmelik, Mercedes-Benz Group içerisinde AB/AEB'den gelen kişisel verilerin işlenmesi için bağlayıcı kurallar öngörmektedir. Bunlar AB/AEB dışındaki kişisel verilerin korunması için uygun garantiler ve Mercedes-Benz Group için bağlayıcı olan şirket kuralları ("Binding Corporate Rules Controller – BCR-C") oluşturmaktadır.

2 Uygulama alanı

Bu AB veri koruma yönetmeliği Mercedes-Benz Group AG, Mercedes-Benz Group AG tarafından kontrol edilen grup şirketleri (bundan sonra **grup şirketleri**) ve çalışanları ve yönetim organlarının üyeleri için geçerlidir. Bu bağlamda, kontrol edilen, Mercedes-Benz Group AG'nin doğrudan ya da dolaylı olarak oy çokluğuna sahip olması, yönetimde çoğunluğa sahip olması veya bir anlaşma yoluyla bu yönetmeliğin benimsenmesini talep edebileceği anlamına gelir.

Yönetmelik, kişisel verilerin tamamen veya kısmen otomatikleştirilmiş bir şekilde işlenmesi ve ayrıca ulusal yasa geçerlilik alanını genişletmediği sürece veri sistemlerinde otomatikleştirilmemiş işleme için geçerlidir. Almanya'da bu yönetmelik matbu tüm çalışan verileri[1] için de geçerlidir.

Yönetmelik, Mercedes-Benz Group için AB menşeli kişisel verilerin işlenmesi için tutarlı ve bağlayıcı şirket kuralları oluşturmaktadır ("Binding Corporate Rules – BCR").

[1] Bu yönetmelikte salt dilin basitleştirilmesi amacıyla sadece eril hitap şekli kullanılacaktır. İçerik olarak her durumda tüm cinsel kimlikler kastedilmektedir.

Yönetmelik kişisel verilerin işlemesi için geçerlidir:

- (a) şubeleri bu yönetmeliğin genişletilebileceği AB/AEB içerisinde veya başka bir ülkede bulunan grup şirketlerine ve bağlı şirketlerine ("AB/AEB'de bulunan şirketler") ait veriler,
- (b) gerçek kişilere ait malları veya hizmetleri AB/AEB içerisinde sundukları ve/veya AB/AEB içerisindeki gerçek kişilerin davranışlarını denetledikleri sürece AB/AEB dışında şubesi bulunan grup şirketlerine ("AB/AEB için teklifleri olan üçüncü ülke şirketleri") ait veriler veya
- (c) kişisel verileri, a) veya b) uyarınca yönetmeliğin geçerli olduğu şirketlerden doğrudan veya dolaylı olarak almış olan veya bunlara ifşa eden AB/AEB dışında şubeleri bulunan grup şirketlerine ("AB/AEB'den veriler alan üçüncü ülke şirketleri") ait veriler.

Yönetmelik kişisel verilerin işlemesi için geçerlidir:

- AB/AEB merkezli şirketler
- AB/AEB için teklifleri olan üçüncü ülke şirketleri
- AB/AEB'den veriler alan üçüncü ülke şirketleri.

Verilen AB/AEB dışında işlenmesi, bu yönetmeliğin devamında verilerin bir üçüncü ülkede işlenmesi olarak adlandırılmaktadır.

Üçüncü ülke şirketleri tarafından işlemeye katılan veya buna tabi olan grup şirketleri *"AB veri koruma yönetmeliğine bağlı olan grup şirketlerinin listesi"* adlı aynı zamanda geçerli düzenlemede belirtilmiştir.

Bu yönetmelik, AB/AEB dışındaki ülkelere genişletilebilir. Tüzel kişilere ait verilerin kişisel verilerle aynı şekilde korunduğu ülkelerde bu yönetmelik, tüzel kişilerin verileri için geçerli olduğu şekilde geçerlidir.

3 Mercedes-Benz Group içerisinde yasal bağlayıcılık

Bu yönetmeliğin düzenlemeleri uygulama alanında faaliyet gösteren tüm grup şirketler için bağlayıcı talimatlardır. Grup şirketleri ve ayrıca bunların yönetimi ve çalışanları bu nedenle geçerli AB talimatları ve ulusal veri koruma yasalarının yanı sıra bu yönetmeliğe uyulmasından sorumludur.

Grup şirketleri, yasal gereksinimlere bağlı olarak kendi başlarına bu yönetmeliğin kapsamı dışında yaptırımlar uygulayamazlar.

4 Yasal gereksinimlere istinaden

Bu yönetmelik, AB talimatlarının ve ulusal yasaların yerine geçmez. Ulusal veri koruma yasalarını tamamlamaktadır. AB yasaları gibi ulusal yasaların kişisel veriler için daha yüksek bir koruma düzeyi öngördüğü durumlarda, söz konusu yasalar bu yönetmeliğin hükümlerinden üstün olacaktır. Bu yönetmeliğin içeriği ilgili ulusal yasalar olmadığında da dikkate alınmalıdır. Üçüncü taraf ülke programlarının izlenmesi ve raporlanması 16. bölümde açıklanmaktadır.

Bu yönetmeliğe uyulması ulusal yasaların ihlal edilmesine neden olacaksa veya ulusal yasalara göre bu yönetmelikle ilgili farklı düzenlemeler gerekiyorsa bu, veri koruma yasası takibi kapsamında veri

koruma için grup yetkilisine ve merkezi Compliance organizasyonuna bildirilmelidir. Ulusal mevzuat ve bu yönetmelik arasında uyuşmazlıklar durumunda veri koruma için grup yetkilisi ve merkezi Compliance organizasyonu bu yönetmeliğin amacına uygun olan pratik bir çözüm bulmak için ilgili grup şirketi ile birlikte çalışacaktır.

5 Kişisel verilerin işlenmesi ile ilgili genel temel kurallar

5.1 Yasallık

Kişisel veriler yasalara uygun ve iyi niyet doğrultusunda toplanmalı ve işlenmelidir. Verilerin işlenmesi yalnızca ilgili işleme için yeterli bir yasal dayanak olduğu sürece gerçekleştirilebilir. Bu, grup şirketleri arasındaki veri işleme için de geçerlidir. Hem aktaran hem de alan şirketin Mercedes-Benz Group'a ait olması gerçeği tek başına veri işlemeyi haklı kılmaz.

Kişisel verilerin herhangi bir şekilde işlenmesi yeterli bir yasal dayanak gerektirir.

Kişisel verilerin işlemesine Madde 5.2 veya 5.3 altındaki onay durumlarından biri mevcut olduğunda izin verilir. Bu tarz bir onay durumu kişisel verilerin işlenmesine yönelik amaç asıl amaca göre değiştiğinde de gereklidir.

5.2 Müşteri ve ortak verilerinin yasal dayanağı

5.2.1 Sözleşmesel bir ilişki için veri işleme

İlgili kişinin, müşterinin veya ortağın kişisel verileri bir sözleşmenin gerekçelendirilmesi, gerçekleştirilmesi ve sonlandırılması için işlenebilir. Bu, sözleşme amacı doğrultusunda olduğu sürece müşteri veya ortak danışmanlığını da kapsamaktadır.

Müşteri ve ortak verileri, bir sözleşmenin gerekçelendirilmesi, gerçekleştirilmesi ve sonlandırılması için ve sözleşme hazırlığı kapsamında işlenebilir.

Bir sözleşmenin ön şartlarında tekliflerin hazırlanması, satış başvurularının hazırlanması ya da ilgili kişinin sözleşmenin yürürlüğe girdikten sonraki isteklerinin karşılanması amacıyla kişisel bilgilerin kullanılmasına izin verilir. Sözleşmenin hazırlanması aşamasında ilgili kişilerle ilettikleri bilgiler ile ilgili olarak iletişime geçilir. Bununla birlikte ilgili kişiler tarafından belirtilen sınırlandırmalara uyulmalıdır.

5.2.2 Reklam amaçlı veri işleme

Müşteri ve ortak verilerinin sadece reklam amaçlı toplanması durumunda veri işlemenin öncesinde ilgili kişinin onayı gereklidir.

İlgili kişi bir grup şirketine bilgi talebi için başvurduğunda (örn. bir ürün ile ilgili bilgi materyali gönderilmesi talebi), bu talebi karşılamak amacıyla verilerin işlenmesine izin verilir. Müşteri bağlama ve reklam uygulamaları başka yasal ön koşullar gerektirir. Kişisel bilgilerin reklam veya pazar ve düşünce araştırma amacıyla kullanımına, verilerin esas toplanma amacı bu amacı da içerdiği sürece izin verilir. İlgili kişi önceden verilerinin reklam amaçlı işlenmesi hakkında bilgilendirilmelidir. Veriler sadece reklam amaçlı toplandığı sürece ilgili kişi verilerini isteğe bağlı olarak verebilir. İlgili kişi verilerin bu amaçla gönüllülük esasına göre verildiği konusunda bilgilendirilmelidir. İletişim kapsamında ilgili kişinin onayı alınmalıdır. İlgili kişi onay çerçevesinde elektronik bildirimler ve telefon gibi mevcut iletişim kanalları arasından seçim yapabilir (onay için bkz. Madde 5.2.3). İlgili kişi verilerinin reklam amaçlı kullanımına izin vermediğinde, verilerin bu amaçla kullanımına ve değerlendirilmesine izin verilmez ve bu amaç için kısıtlanmalıdır veya engellenmelidir. Ayrıca bazı ülkelerdeki verilerin reklam amaçlı kullanımı konusundaki mevcut sınırlandırmalara dikkat edilmelidir.

5.2.3 Veri işleme için muvafakat

Veri işleme ilgili kişinin isteği sonucunda gerçekleşebilir. Bu talepten önce ilgili kişi bu AB veri koruma yönetmeliğine göre bilgilendirilmelidir. Kanıt teşkil etmesi amacıyla düzenli olarak yazılı ya da elektronik olarak onay beyanı alınmalıdır. Örneğin telefonla danışma gibi bazı durumlarda talep sözlü olarak da iletilebilir. İletimleri ise belgelenmelidir.

5.2.4 Yasal izinler veya zorunluluk sebebiyle veri işleme

Kişisel bilgiler, ancak ulusal yasalar veri işlemlerini talep ediyorsa, gerektiriyorsa ya da bu işlemlere izin veriyorsa işlenebilir. Veri işlemenin tür ve kapsamı yasal olarak izin verilen veri işleme için gerekli olmalı ve bu yasalara uygun yapılmalıdır.

Müşteri ve ortak verilerinin işlenmesine ulusal yasal talimatlara uyulması için izin verilir.

5.2.5 Meşru menfaatler sebebiyle veri işleme

Kişisel veriler, ilgili bir kişinin hakkının aranması için gerekli olduğunda da işleme tabi tutulabilir. İlgili kişilerin hakları genellikle yasal (örn. açık gerekliliklerin yürürlüğe alınması) ya da ekonomiktir (örn. sözleşme ihlallerinden kaçınma). Münferit durumlarda ilgili kişinin verilerinin korunmasına yönelik hakları, verilerin işlenmesindeki meşru menfaatleri kısıtladığında bir meşru menfaat sebebiyle veri işleme gerçekleştirilemez. Korunması gereken menfaatler her işleme için kontrol edilmelidir.

Müşteri ve ortak verilerinin bir meşru menfaat doğrultusunda işlenmesine, ilgili kişinin koruması gereken menfaatleri kısıtlanmadığı sürece izin verilir.

5.3 Çalışan verileri için yasal dayanak

5.3.1 İş ilişkileri ile ilgili verilerin işlenmesi

İş ilişkisinin gerekçelendirilmesi, gerçekleştirilmesi ve sonlandırılması için gerekli olan kişisel veriler işlenebilir. Bir iş ilişkisinin gerekçesi ile ilgili karar için iş başvurusunda bulunan kişilerin kişisel verileri işlenebilir. Reddedildikten sonra adaya ait bilgiler, aday daha sonraki bir seçim aşaması için verilerin kaydedilmesi talebinde bulunmadığı sürece durumun ispat edilmesini gerektirebilecek zaman aşımı süreleri göz önünde bulundurularak silinir. Verilerin daha sonraki başvuru işlemlerinde ya da diğer şirketlere başvuru amacıyla aktarılmasından önce de onay gereklidir. Mevcut bir iş ilişkisi durumunda verilerin işlenmesi, daha sonraki onay sebeplerinden biri veri işleme ile çakışma yaratmadığı sürece her zaman iş ilişkisi ile ilgili olmalıdır.

Çalışan verileri iş ilişkisinin gerekçelendirilmesi, gerçekleştirilmesi ve sonlandırılması için ve iş başvurusu kapsamında işlenebilir.

İş ilişkisi hazırlığı sırasında veya mevcut bir iş ilişkisi durumunda üçüncü tarafta iş başvurusu yapan kişi hakkında daha fazla bilgi toplanması gerektiği durumda ilgili ulusal yasal gereksinimler dikkate alınmalıdır. Şüpheli durumlarda izin verildiği sürece ilgili kişinin onayı alınmalıdır.

İş ilişkisi bağlamında olan ancak aslında iş ilişkisinin gerekçelendirilmesi veya sonlandırılması için kullanılmayan (çalışan verileri) kişisel verilerin işlemesi için aşağıda belirtilen yasal dayanaklardan biri mevcut olmalıdır.

5.3.2 Yasal izinler veya zorunluluk sebebiyle veri işleme

Çalışan verileri, ancak ulusal yasalar verilerin işlenmesini talep ediyorsa, gerektiriyorsa ya da bu işlemlere izin veriyorsa işlenebilir. Veri işlemenin tür ve kapsamı yasal olarak izin verilen veri işleme için gerekli olmalı ve bu yasalara uygun yapılmalıdır. Hukuki bir mutabakat aralığı olması durumunda çalışanın korunması gereken hakları göz önünde bulundurulmalıdır.

5.3.3 Verilerin işlenmesi için toplu anlaşma

Bir veri işleme, sözleşme imzalandıktan sonra amacının ötesine geçiyorsa, bu duruma ancak verilerin işlenmesi bir toplu anlaşma tarafından meşrulaştırıldığında izin verilir. Kurallar arzu edilen veri işleme işleminin somut amacına hizmet etmelidir ve AB talimatları ve ulusal yasalar çerçevesinde modellenebilir.

Çalışan verileri, bir toplu anlaşma ile izin verildiği sürece işlenebilir.

5.3.4 Veri işleme için muvafakat

Çalışan verilerinin işlenmesi ilgili kişinin onayı doğrultusunda gerçekleşebilir. Onay beyannameleri serbest biçimde verilebilmelidir. Onay verilmemesi çalışan için dezavantajlara neden olmamalıdır. Gönüllü olarak verilmeyen onayların bir geçerliliği yoktur. Kanıt teşkil etmesi amacıyla düzenli olarak yazılı ya da elektronik olarak onay beyanı alınmalıdır. Koşullar buna müsaade etmediği durumlarda onay sözlü olarak verilebilir. Onayın verilmesi her durumda kurallara uygun bir

şekilde belgelenmelidir. Bu talepten önce ilgili kişi bu AB veri koruma yönetmeliğine göre bilgilendirilmelidir.

5.3.5 Meşru menfaatler sebebiyle veri işleme

Çalışan verileri, grup şirketinin haklarının aranması için gerekli olduğunda da işlenebilir. Çalışan kişilerin hakları genellikle yasal (örn. tazminat ödemesi ya da yasal hakların korunması) ya da ekonomiktir (örn. ticari işlemlerin hızlandırılması, şirketin değerlendirilmesi). Korunması gereken menfaatlerin mevcut olup olmadığı her veri işleme öncesinde kontrol edilmelidir. Kişisel verilerin meşru bir menfaat temelinde işlenmesi, çalışanın korunması gereken menfaatleri, verilerin işlenmesindeki menfaatten ağır basmıyorsa gerçekleştirilebilir.

Çalışan verilerinin bir meşru menfaat doğrultusunda işlenmesine, ilgili kişinin korunması gereken menfaatleri kısıtlanmadığı sürece izin verilir.

İş ilişkisinin gerçekleştirilmesi dışında (örn. performans kontrolü) çalışanlara ait verilerin işlenmesini gerektiren kontrol önlemleri yalnızca yasal bir zorunluluk bulunduğunda ya da açık bir sebep bulunduğunda alınmalıdır. Haklı bir sebep olsa dahi kontrol önleminin ölçülü olup olmadığı kontrol edilmelidir. Bu amaçla, grup şirketinin kontrol önleminin uygulanmasındaki meşru menfaatleri (örn. yasal düzenlemelere ve şirket içi kurallara uygunluk), önlemi hariç tutmada etkilenen çalışanın muhtemel meşru menfaatine karşı tartılmalıdır. Önlemler ancak somut durumlarda uygunsa uygulanabilir. Grup şirketinin bu hakkı ve çalışanın korunması gereken hakkı, her önlemden önce belirlenmeli ve belgelenmelidir. Ayrıca gerektiğinde geçerli hukukun diğer gereksinimleri (örn. çalışan tarafının temsilcisinin ortak karar alma hakkı ve ilgili kişinin bilgi alma hakkı) göz önünde bulundurulmalıdır.

5.4 Özellikle korunması gereken verilerin işlenmesi

Özellikle korunması gereken kişisel verilerin işlemesi yasal olarak ön görüldüğü veya izin verildiği sürece gerçekleştirilebilir. Bu tarz verilerin grup şirketi tarafından işlenmesine özellikle ilgili kişi işlemeye onay verdiğinde, ilgili kişiye karşı yasal hakları kullanabilmek, uygulamak veya savunmak için işleme zorunlu olduğunda veya iş hukuku veya sosyal hukuk kapsamında haklara ve yükümlülüklere uymak için izin verilebilir.

Özellikle korunması gereken verilerin işlenmesi, yasal izin veya ilgili kişinin açık onayını gerektirir.

Özellikle korunması gereken kişisel verilerin işlenmesi planlanıyorsa, önceden veri koruma için grup yetkilisi bilgilendirilmelidir.

5.5 Otomatikleştirilmiş münferit durum kararları (varsa Profiling dahil)

İlgili kişi, ancak sözleşmenin tamamlanması veya gerçekleştirilmesi için gerekli olması veya ilgili kişinin onayı olması durumunda, kendisi üzerinde yasal veya benzer olumsuz etkileri olan münhasıran otomatik bir karara tabi tutulabilir. Münferit durumlarda bu otomatikleştirilmiş karar, Profiling, yani bireysel kişilik özelliklerinin (ör. kredi itibarı) değerlendirildiği kişisel verilerin işlenmesi ile birleştirilebilir. Bu durumda, ilgili kişi, otomatikleştirilmiş bir münferit kararın durumu ve

Otomatikleştirilmiş münferit durum kararları ve Profiling, yalnızca katı koşullar altında mümkündür.

sonucu hakkında bilgilendirilmeli ve sorumlu bir kişi tarafından bireysel bir kontrol mümkün olmalıdır.

5.6 Bilgi verme yükümlülüğü/şeffaflık

Sorumlu uzmanlık alanı, ilgili kişileri, DSGVO Madde 13 ve 14 uyarınca kişisel verilerinin işlenmesine ilişkin amaçlar ve koşullar hakkında bilgilendirmelidir. Bilgilendirme net, şeffaf, anlaşılır ve kolay erişilebilir bir şekilde ve sade ve kolay bir dil ile gerçekleştirilmelidir. Veri koruma için grup yetkilisinin ve Data Compliance'ın talimatları dikkate alınmalıdır. Bu bilgi genel olarak kişisel verilerin ilk toplandığı sırada sağlanmalıdır. Grup şirketi kişisel verileri üçüncü bir kişiden aldığı sürece bilgiyi, veriler talep edildikten sonra ilgili kişiye uygun bir zaman içerisinde sağlamalıdır. Ancak bu, aşağıdaki durumlarda geçerli değildir:

- ilgili kişi halihazırda bu bilgilere sahipse
- bu bilgilerin verilmesi mümkün olmadığında veya
- aşırı bir uğraş gerektirmesi durumunda.

İlgili kişi, kişisel verilerinin işlenmesinin amaçları ve koşulları hakkında bilgilendirilmelidir.

5.7 Amaca uygunluk

Kişisel veriler, yalnızca verilerin toplanmasından önce tanımlanan meşru amaç için işlenebilir. İşleme amacında sonraki değişikliklere, yalnızca işlemenin kişisel verilerin ilk toplandığı amaçlarla uyumlu olması koşuluyla izin verilir.

Kişisel veriler, yalnızca verilerin toplanmasından önce tanımlanan meşru amaç için işlenebilir.

5.8 Verilerin minimizasyonu

Kişisel verilerin herhangi bir şekilde işlenmesi, verilerin yasal olarak işlendiği amaçlara ulaşmak için gerekli olanla hem nicel hem de nitel olarak sınırlandırılacak şekilde tasarlanmalıdır. Bu, veri toplama kapsamında da dikkate alınmalıdır. Amaç izin verdiği ve uğraş izlenen hedefle orantılı olduğu sürece, anonimleştirilmiş veya istatistiksel veriler kullanılmalıdır.

Kişisel verilerin işlenmesi, amaçlara ulaşmak için gerekli olanlarla sınırlı olmalıdır.

5.9 Verilerin doğruluğu

Kaydedilen kişisel veriler konu bakımından doğru ve gerekirse en güncel durumda olmalıdır. Sorumlu uzmanlık alanı, yanlış veya eksik verilerin silindiğinden, düzeltildiğinden, tamamlandığından veya güncellendiğinden emin olmak için uygun önlemler almalıdır.

5.10 Privacy by Design & Privacy by Default

"Privacy by Design" ilkesi, veri koruma ilkelerini, daha en baştayken konsept oluşturma ve teknik tasarım aşamasında iş modellerinin/proseslerinin spesifikasyonlarına ve mimarisine ve ayrıca veri işlemeye yönelik BT sistemlerine dahil etmek için uzmanlık alanlarının teknolojinin en güncel durumuna göre dahili stratejiler belirlemesini ve tedbirler almasını amaçlamaktadır. "Pirvacy by Design" ilkesine göre kişisel verilerin işlemesine yönelik işlemler ve sistemler, başlangıç ayarları ilgili amacın yerine getirilmesi için gerekli veri işleme işlemleri ile kısıtlı olacak şekilde tasarlanmış olmalıdır ("Privacy by

Veri koruma ilkeleri, iş modellerinin, süreçlerin ve BT sistemlerinin mimarisine entegre edilmelidir.

Default" ilkesi). Bu, veri işleme kapsamını, kayıt süresini ve erişilebilirliği kapsamaktadır. Aşağıdaki şekillerde daha fazla önlem gerekebilir:

- kişiselleştirilmiş verilerin en kısa süre içerisinde kodla şifrelenmesi
- kişisel verilerin fonksiyonlarına ve işlenmesine yönelik şeffaflığın oluşturulması
- ilgili kişiye kişisel verilerin işlenmesi ile ilgili karar verme imkanı sunulması
- işlem veya sistem operatörlerinin güvenlik fonksiyonları oluşturma ve iyileştirme durumunda olması.

Her grup şirketi, yukarıda belirtilen ilkelere her zaman uyulmasını sağlamak için işleme faaliyetlerinin tüm yaşam döngüsü boyunca uygun teknik ve organizasyonel önlemleri uygular ve yürütür.

5.11 Silme ve anonimleştirme

Kişisel veriler, verilerin işlendiği amaç için gerekli olduğu sürece saklanmalıdır.

Kişisel veriler, verilerin işlendiği amaç için gerekli olduğu sürece saklanmalıdır. Bu, başka saklama yükümlülükleri olmadığı sürece kişisel verilerin işleme amacı yerine getirildiğinde veya başka nedenlerden dolayı geçersiz olduğunda silindiği veya anonimleştirildiği anlamına gelir. Münferit işlemlerden sorumlu kişiler işlemleri için silme ve anonimleştirme rutinlerinin uygulanmasını sağlamalıdır. Her sistemin kendine ait manuel veya otomatik bir silme rutini olmalıdır. Kişisel referansın silinmesi veya kaldırılması için veri sahiplerinden gelen silme talepleri, sistemlerde teknik olarak mümkün olmalıdır. Mercedes-Benz Group AG'nin silme rutinlerinin uygulanmasına yönelik belirttiği talimatlar (yazılım araçları, silme taleplerinin uygulanması için yardım, dokümantasyon talepleri gibi) dikkate alınmalıdır.

5.12 Verilerin işlenmesinde güvenlik

Teknik ve organizasyonel önlemlerle veri işleme güvenliği sağlanmalıdır.

Kişisel veriler, yetkisiz erişime ve yasa dışı işlenme veya ifşaya ve ayrıca istem dışı kaybolmaya, değiştirilmeye veya imha edilmeye karşı korunmalıdır. Verilerin işlenmesi için özellikle yeni BT sistemleri olmak üzere yeni işlemler kullanmaya başlamadan önce kişisel verilerin korunması için teknik ve organizasyonel önlemler belirlenir ve uygulanır. Bu önlemler en güncel durumda olmalıdır, işleme riskine ve verilerin koruma ihtiyacına dayanmalıdır.

Veri koruma sonuçlarının değerlendirilmesinin ve yöntem kaydının bir parçası olarak, veri korumasına ilişkin teknik ve organizasyonel önlemler sorumlu kişiler tarafından belgelendirilmelidir.

Özellikle ilgili uzmanlık alanı, Business Information Security Officer (BISO), bilgi güvenliği görevlisi (ISO) ve veri koruma ağına danışmalıdır. Kişisel verileri korumaya yönelik teknik ve organizasyonel önlemlere yönelik gereksinimler, grup çapında bilgi güvenliği yönetiminin bir parçasıdır ve teknik gelişmelere ve organizasyonel değişikliklere sürekli olarak uyarlanmalıdır.

5.13 (Diğer)Aktarımlar

Kişisel verilerin grup şirketleri dışındaki alıcılara veya grup şirketleri içindeki alıcılara aktarılması, bu Madde 5 kapsamında kişisel verilerin işlenmesi için kabul edilebilirlik şartlarına tabidir. Verilerin alıcısı bir sözleşme ile aldığı verileri sadece belirlenen amaçlarla kullanacağını taahhüt etmelidir. Ayrıca, bölüm 15 kişisel verilerin AB/AEA'dan üçüncü bir ülkeye aktarılması için de geçerlidir.

Madde 5'te belirtilen tüm yükümlülükler ilgili kişi için üçüncü kişi lehinedir.

6 Veri koruma sonuçlarının değerlendirilmesi

Grup şirketleri yeni veri işleme yöntemleri sunulduğunda veya mevcut veri işleme yönteminde önemli bir değişiklik yapıldığında verilerin işlenmesinden önce özellikle yeni teknolojilerin kullanımı ile gerçekleştirilen bu veri işlemenin, ilgili kişinin özel hayatına yönelik yüksek bir risk barındırıp barındırmadığını analiz etmektedir. Bu durumda veri işlemenin türü, kapsamı, bağlamı ve amacı dikkate alınmalıdır. Sorumlu uzmanlık alanı, risk analizi kapsamında, planlanan veri işlemenin kişisel verilerin korumasına yönelik etkileri açısından bir değerlendirme gerçekleştirmektedir (veri koruma sonuçlarının değerlendirilmesi). Veri koruma sonuçlarının değerlendirilmesi gerçekleştirildikten ve risklerin azaltılması için uygun tedbirlerin uygulanmasından sonra ilgili kişinin haklarına ve özgürlüklerine yönelik yüksek bir risk söz konusuysa veri koruma için grup yetkilisi, ilgili veri koruma denetim makamına danışabilmesi için bilgilendirilmelidir. Mercedes-Benz Group AG'nin veri koruma sonuçlarının değerlendirilmesinin gerçekleştirilmesi için belirttiği talimatlar (yazılım gereçleri, değerlendirmenin gerçekleştirmesine yönelik talimatlar) dikkate alınmalıdır.

Veri koruma sonucu değerlendirmesinde, planlanan işlemenin kişisel verilerin korumasına etkisi değerlendirilmektedir.

7 Veri işleme yöntemlerinin dokümantasyonu

Her bir grup şirketi kişisel verilerin işlendiği yöntemleri bir yöntem kaydında dokümante etmelidir. Yöntem kaydı, elektronik biçimde de gerçekleştirilebilen yazılı şekilde yapılmalıdır ve talep edilmesi halinde veri koruma denetim makamına sunulmalıdır. Mercedes-Benz Group AG'nin dokümantasyon ile ilgili belirttiği talimatlar (yazılım gereçleri, dokümantasyon talimatları) dikkate alınmalıdır.

Yöntem kaydı üzerinden veri işleme yöntemleri dokümante edilir.

8 İş emri üzerine işleme

8.1 Genel hususlar

Görevlendirilen bir taraf, kişisel verileri görevlendirenin adına ve talimatı üzerine işlediğinde bir iş emri işlemi söz konusudur. Bu durumlarda hem görevlendiren harici taraflar ile hem de Mercedes-Benz Group içerisinde, grup şirketleri arasında geçerli yasal gereksinimler uyarınca bir iş emri işlemi ile ilgili bir anlaşma yapılmalıdır (örn. "iş emrinin işleme alınması

Bir iş emrinin işlenmesi, görevlendiren ve görevlendirilen arasında yazılı bir anlaşma gerektirir.

ile ilgili anlaşma" şablonu). Bu sırada veri işlemenin doğru bir şekilde gerçekleştirilmesi için tüm sorumluluk görevlendiren taraftadır.

Madde 8.3'teki düzenlemeler ayrıca harici görevlendirenin grup şirketi olmaması durumunda da uygulanır.

8.2 Görevlendiren için düzenlemeler

İş emri verilirken aşağıda belirilen talimatlara uyulmalı ancak görevlendiren uzmanlık bölümü bunların uygulandığından emin olmalıdır:

- Görevlendirilen şirket, gerekli teknik ve organizasyonel koruma önlemlerini sağlamak için uygunluğuna göre seçilmelidir.
- Veri koruma için grup yetkilisi tarafından sunulan sözleşme standartları dikkate alınmalıdır.
- İş emri yazılı veya elektronik olarak verilmelidir. Veri işleme talimatları ve görevlendiren ile görevlendirilen şirketin sorumlulukları dokümante edilmelidir.

Görevlendiren şirket, verilerin işlenmesine başlanmadan önce uygun bir kontrol ile, görevlendirilen şirketin önceden belirtilen yükümlülükleri yerine getirdiğinden emin olmalıdır. Mercedes-Benz Group AG'nin bununla ile ilgili belirttiği talimatlar (yazılım gereçleri, değerlendirmenin gerçekleştirilmesi için talimatlar, sözleşme taslağı) dikkate alınmalıdır. Görevlendirilen bir şirket, veri gizliliği gerekliliklerine uyduğunu özellikle uygun bir sertifikasyon ile dokümante edebilir. Verilerin işlenmesinin riskine bağlı olarak kontroller sözleşme süresi boyunca düzenli olarak tekrarlanmalıdır.

8.3 Görevlendirilenler ile ilgili grup içerisindeki düzenlemeler

Görevlendirilen kişisel verileri sadece görevlendirenin talimatları kapsamında işleyebilir.

Görevlendirilen şirketler, kişisel verilerin kendi emrinde işlenmesi için diğer grup şirketlerini veya Üçüncü Tarafları ("**alt yükleniciler**") sadece görevlendiren şirketten önceden onay aldıktan sonra görevlendirebilir. Onay, yalnızca görevlendirilenin alt yükleniciye (sözleşmeden veya benzer şekilde yasal olarak bağlayıcı) grup şirketine ve ilgili kişilere karşı bu yönetmeliğe uygun olarak uyması gereken aynı veri koruma yükümlülüklerinin yanı sıra uygun teknik bilgileri ve organizasyonel koruyucu önlemleri empoze etmesi durumunda verilir. Onayın şekli ve ayrıca alt yüklenici ilişkisinde değişiklikler durumunda bilgilendirme yükümlülükleri hizmet sözleşmesinde düzenlenmelidir.

Görevlendirilenler, özellikle bunu kanıtlamak için gerekli tüm bilgileri sağlayarak, görevlendirilene uygulanan veri koruma düzenlemelerine uyma konusunda görevlendireni yeterince desteklemekle yükümlüdür; bu özellikle aşağıdaki hususları korumak için geçerlidir:

- Madde 5 uyarınca işleme için genel ilkeler
- Madde 10 uyarınca ilgili kişi hakları

- Madde 12 uyarınca görevlendirenin bilgilendirme yükümlülükleri
- Madde 8 uyarınca görevlendiren ve görevlendirilen için düzenlemeler
- ve ayrıca taleplerin ele alınması ve denetim makamları tarafından incelemeler.

Geçerli standartlar veya yasal düzenlemeler, görevlendirilenin talimatın aksine bir işleme yapmasını şart koştuğunda veya bu yasal düzenlemeler görevlendirilenin bu yönetmelikteki veya iş emri işlemeye yönelik anlaşmadaki yükümlülüklerini yerine getirmesini engellediğinde görevlendirilen bunu, ilgili yasal düzenleme yasaklamadığı sürece görevlendirene derhal bildirir. Bu, görevlendirilenin başka nedenlerle görevlendirenin talimatlarına uymaması durumunda geçerlidir. Bu durumda görevlendiren verilerin aktarımını durdurma ve/veya iş emri işlemesi ile ilgili sözleşmeyi sonlandırma hakkına sahiptir.

Görevlendirilenler, başka nedenlerle yasaklanmadığı sürece, kişisel verilerin bir makam tarafından ifşa edilmesine ilişkin yasal olarak bağlayıcı herhangi bir talebi görevlendirene bildirmekle yükümlüdür.

Hizmetin sağlanmasının sona ermesi üzerine, görevlendirilen, görevlendirenin takdirine bağlı olarak, görevlendiren tarafından sağlanan tüm kişisel verileri silmeli veya iade etmelidir.

Görevlendirilenler görevlendireni ve varsa bunun arkasındaki görevlendireni derhal ilgili kişilerin geçerli kılınan hakları, başvuruları veya şikayetleri hakkında bilgilendirmekle yükümlüdür.

Grup içerisindeki görevlendirenler, grup dışı görevlendirilenleri de yukarıdaki düzenlemelere uymaya mecbur etmelidir.

Görevlendirilenin görevlendiren karşısındaki spesifik yükümlülükleri ilgili kişi için üçüncü taraf lehinedir.

9 Ortak sorumluluk

Kişisel veri işleme araçlarını ve amaçlarını birden fazla grup şirketinin ortak bir şekilde belirlemesi durumunda (varsa bir veya birden fazla üçüncü taraf ile birlikte) (ortak sorumlu makam/ Joint Controller), şirketler verilerini işledikleri ilgili kişi karşısında görevleri ve sorumluluklarının belirlendiği bir anlaşma yapmalıdır. Bu sırada grup yetkilileri tarafından veri koruması için sunulan sözleşmesel talimatlar dikkate alınmalıdır.

Veri işlemenin araç ve amaçları birkaç grup şirketi tarafından ortaklaşa belirlenirse, bu "ortak sorumluluk"tan sorumlu olanlar arasında yazılı bir anlaşma yapılması gerekir.

10 İlgili kişiler için uygulanabilir haklar

Madde 10'da belirtilen ilgili kişilerin tüm hakları ve grup şirketlerinin yükümlülükleri ilgili kişi için üçüncü kişi lehinedir.

Madde 10'a göre yapılan başvurular ve şikayetler bir ay içerisinde yanıtlanmalıdır. Başvuruların karmaşıklığı ve sayısı dikkate alınarak bu süre bir aydan en fazla iki aya kadar uzatılabilir. Ancak bu durumda ilgili kişi uygun bir şekilde bilgilendirilmelidir.

10.1 İlgili kişinin hakları

AB/AEB'deki bir ilgili kişi sorumlu ilgili grup şirketi veya görevlendirilen taraf olması durumunda görevlendiren karşısında aşağıda belirtilen haklara sahiptir. Bunlar AB yasasında ayrıntılı olarak belirlenmiştir:

- kişisel verilerin işlenmesine yönelik koşullar hakkında bilgi edinme hakkı. Bu tür bilgilere dair veri koruma için grup yetkilisinin talimatları dikkate alınmalıdır.
- verilerin hangi şekilde işlendiğine ve hangi haklara sahip olunduğuna dair bilgi edinme hakkı. İş ilişkisinde iş verenin belgelerinde ilgili iş yasası uyarınca özel inceleme hakları tanınmışsa (örn. sicil dosyası), bu haklar sabit kalır. Talep üzerine, üçüncü kişilerin çıkarları bununla çelişmediği sürece, ilgili kişiye kişisel verilerinin bir kopyası (gerekirse makul bir ücret karşılığında) verilir.
- yanlış veya eksik ise kişisel verileri düzeltme veya tamamlama hakkı.
- onayını geri çekmesi veya verilerin işlenmesi için yasal dayanağın eksik olması veya ortadan kalkması durumunda verilerini silme hakkı. Aynı durum, veri işlemlerinin amacı zaman aşımı ya da diğer nedenlerden ötürü geçersiz olduğunda da geçerlidir. Silme işlemiyle çelişen mevcut saklama yükümlülükleri ve korunması gereken menfaatler dikkate alınmalıdır.
- doğruluğunu inkar etmesi veya verilerin artık grup şirketi tarafından talep edilmemesi durumunda, yalnızca ilgili kişinin yasal talepleri için verilere ihtiyaç duyması halinde verilerinin işlenmesini kısıtlama hakkı. İlgili kişi, aksi takdirde verileri silmek zorunda kalırsa veya ilgili kişinin itirazını incelerse, grup şirketinden verilerinin işlenmesini kısıtlamasını da talep edebilir.
- işleme otomatik prosedürler kullanılarak gerçekleştirildiği ve bu teknik olarak mümkün olduğu sürece onaya dayalı olarak veya kendisi ile akdedilen veya askıda olan bir sözleşme çerçevesinde kendisi ile ilgili ve kendisi tarafından sağlanan kişisel verileri ortak bir dijital formatta alma ve bunu üçüncü bir kişiye iletme hakkı.
- herhangi bir zamanda doğrudan pazarlamaya itiraz etme hakkı. Uygun bir onay ve itiraz yönetimi sağlanmalıdır.
- kişisel durumundan kaynaklanan sebepler varsa, grup şirketlerinin veya üçüncü şahısların üstün çıkarlarının yasal dayanak doğrultusunda işlenmesine itiraz etme hakkı. Grup şirketi, verilerin işlenmesi için menfaatlerinize, haklarınıza ve özgürlüklerinize ağır basan zorlayıcı meşru gerekçeler göstermedikçe veya verilerin işlenmesi yasal hakları geçerli kılmaya, uygulamaya veya savunmaya hizmet etmedikçe, kişisel verilerinizi işlemeyi durdurur. Haklı bir itiraz durumunda veriler silinmelidir.

AB içerisindeki ilgili kişiler şu haklara sahiptir:

- Bilgi alma hakkı
- Bilgilenme hakkı
- Düzeltme hakkı
- Silme hakkı
- Kısıtlandırma hakkı
- Veri aktarma hakkı
- İtiraz hakkı
- Veri koruma için grup yetkilisine veya ilgili denetim makamına şikayette bulunma hakkı.

Ayrıca ilgili kişi üçüncü bir ülkede verileri içe aktaran grup şirketine karşı haklarını kullanma hakkına sahiptir.

10.2 Şikayet yöntemi

İlgili kişiler, bu yönetmeliğin ihlal edildiğini düşünüyorlarsa veri koruma için grup yetkilisine bir şikayette bulunma hakkına sahiptir. Bu tarz şikayetler e-posta üzerinden gönderilebilir (Madde 13.3).

Veri ihracatçısı olarak faaliyet gösteren AB/AEB'deki grup şirketi, kişisel verileri AB/AEB içerisinde toplanan ilgili kişiye, verileri ihraç eden grup şirketi karşısında konunun tespit edilmesi ve bu yönetmelik uyarınca haklarını kullanabilmesi konusunda destek sunacaktır.

Şikayetin haklı bulunması halinde, grup şirketi bu yönetmeliğe uyulmasını sağlamak için uygun önlemleri alacak ve ilgili kişi alınan önlemler ve diğer hakları konusunda bilgilendirecektir. İlgili kişinin grup şirketinin yanıtından memnun kalmaması veya şikayetin reddedilmesi durumunda, ilgili kişi haklarını kullanarak bu karara veya davranışa itiraz etmekte özgürdür ve buna göre bilgilendirilmelidir. Bunun için özellikle mutat meskeninin ya da çalışma yerinin bulunduğu veya olası ihlalin gerçekleştiği ülkede ilgili denetim makamına başvurabilir veya mahkemede dava açabilir (Madde 11.2). Diğer haklar ve sorumluluklar bundan dolayı etkilenmez. Bu dahili şikayet sürecinden bağımsız olarak, ilgili kişiler doğrudan bir denetim makamına şikayette bulunma hakkına sahiptir.

11 Sorumluluk ve yetkili mahkeme

11.1 Sorumluluk düzenlemeleri

Verileri AB/AEB'den alan üçüncü ülke şirketinin, üçüncü ülkede işleme kapsamında bu yönetmeliğe karşı gerçekleştirdiği her türlü ihlalin sorumluluğu, kişisel verileri ilk olarak bir üçüncü ülkede bulunan grup şirketine aktarmış olan AB/AEB merkezli grup şirketi ("veri ithalatçısı") tarafından üstlenilir. Bu sorumluluk, üçüncü ülkelerdeki grup şirketleri tarafından bu yönetmeliğe karşı bir ihlalden doğan yasalara aykırı durumu giderme ve maddi ve manevi zararları karşılama yükümlülüğünü kapsar.

Veri ihracatçısı bu sorumluluktan yalnızca, AB/AEB'den veri alan üçüncü ülke şirketinin zarara neden olan olaydan sorumlu olmadığını kanıtlaması durumunda tamamen veya kısmen muaf tutulur.

11.2 Yetkili mahkeme

İlgili kişi, sorumlu makamın veya görevlendirilen tarafın kayıtlı ofisinin bulunduğu yerdeki veya kendi mutat meskenindeki mahkemelerde dava açabilir.

Veri ihracatçısı, üçüncü bir ülke şirketinin neden olduğu bu yönetmelik ihlallerinin maddi olarak karşılanmasından ve zararların karşılanmasından sorumludur.

Verilerin bir üçüncü ülkede işlenmesi kapsamında bu yönetmeliğe karşı bir ihlalden dolayı hak talep eden ilgili kişi, haklarını hem verileri ithal eden hem de AB/AEB'deki verileri ihraç eden şirketten talep edebilir. Bu nedenle ilgili kişi iddia edilen ihlali ve bundan dolayı doğan hakları sorumlu makamın bulunduğu yerde veya mutat meskeninde bulunan yetkili mahkemelerden ve denetim makamlarından talep edebilir.

Bu maddedeki sorumluluk ve yetkili mahkeme ile ilgili düzenlemeler ilgili kişi için üçüncü taraf lehinedir.

12 Veri koruma vakalarının bildirilmesi

Veri güvenliği düzenlemelerine karşı olası bir ihlal durumunda ("Veri koruma vakası") ilgili grup şirketleri araştırma, bilgilendirme ve tazminat yükümlülüklerine tabidir. Bir veri koruma vakası, kişisel verilerin yasalara uygun olmayan bir şekilde silinmesine, değiştirilmesine, izinsiz ifşa edilmesine veya kullanımına yol açan bir veri güvenliği ihlali olduğunda gerçekleşen bir veri koruma ihlalidir. Bunun gerçek kişilerin hak ve özgürlüklerine yönelik bir riske yol açmasının muhtemel olduğu durumlarda, grup şirketi ilgili ihlali aşırı gecikme olmaksızın ve mümkünse grup şirketinin ihlalden haberdar olmasını izleyen 72 saat içerisinde sorumlu denetim makamına bildirmelidir. Ayrıca ilgili kişiler de hakları ve özgürlükleri için muhtemelen yüksek bir risk barındıran bir veri koruma ihlali durumunda bu veri koruma ihlali hakkında bilgilendirilmelidir. Madde 8.2 uyarınca görevlendirilenler veri koruma vakalarını derhal görevlendirene bildirmekle yükümlüdür.

İlgili kişilerin hakları ve özgürlükleri için yüksek risk oluşturması muhtemel veri koruma ihlalleri, yetkili denetim makamına ve ilgili kişilere bildirilmelidir.

Bir grup şirketinin sorumluluk alanında bir veri koruma vakası belirlenmesi veya olduğundan şüphelenilmesi durumunda her çalışan, bunu Information Security Incident Management prosesi kapsamında Mercedes-Benz Group AG'ye derhal bildirmelidir. Mercedes-Benz Group AG'nin bununla ile ilgili belirttiği talimatlar (yazılım gereçleri, ihbarın gerçekleştirilmesi için talimatlar) dikkate alınmalıdır.

Her bir veri koruma ihlali dokümante edilmelidir ve dokümantasyon talep üzerine denetim makamına sunulmalıdır.

13 Veri koruma organizasyonu ve yaptırımlar

13.1 Sorumluluk

Grup şirketlerinin yönetim organlarının üyeleri, kendi sorumluluk alanlarındaki veri işlemeden sorumludur ve çalışanlarının gerekli veri koruma bilgisine sahip olmalarını sağlamalıdır.

Grup şirketlerinin yönetim organlarının üyeleri, kendi sorumluluk alanlarındaki veri işlemeden sorumludur. Bu nedenle, yasal veri koruma gereksinimlerinin ve bu AB veri koruma yönetmeliğinde yer alan talimatların (örn. ulusal ihbar yükümlülükleri) dikkate alınmasını sağlamakla yükümlüdürler. Organizasyonel, personel ve teknik önlemlerle veri korumasına uygun veri işlemeyi sağlamak, sorumluluğu kapsamında her yöneticinin görevidir. Bu talimatların uygulanması ise ilgili çalışanın sorumluluğundadır. Makamlar tarafından veri koruma kontrollerinde veri koruma için grup yetkilisi derhal bilgilendirilmelidir.

13.2 Farkındalık oluşturma ve eğitim

Yönetim elemanları, kişisel verilere sürekli veya düzenli olarak eriştikleri, verilerin toplanmasına veya kişisel verilerin işlenmesine yönelik gereçlerin geliştirmesine katıldıkları sürece bu yönetmeliğin içeriği ve ele alınması dahil olmak üzere tüm çalışanların gerekli veri koruma eğitimlerini almasını ve bunlara katılmasını sağlamalıdır. Veri koruma için grup yetkilisi ve Data Compliance'ın talimatları dikkate alınmalıdır.

13.3 Organizasyon

Veri koruma için grup yetkilisi talimatlara bağlı değildir.

Veri koruma için grup yetkilisi, görevlerin yerine getirilmesi açısından dahili olarak talimatlara bağlı değildir. Ulusal ve uluslararası veri koruma düzenlemelerinin uyulmasına yönelik görev alır. Bu yönetmelikten sorumludur ve buna uyulmasını denetler. Grup şirketlerinin veri koruma ile ilgili bağlayıcı şirket kuralları için uluslararası bir sertifikalandırma sistemine katılmak istemeleri durumunda bu katılım hakkında veri koruma için grup yetkilisi ile mutabakata varmalıdır.

Veri koruma için grup yetkilisi Mercedes-Benz Group AG yönetim kurulu tarafından atanır ve görevlerini yerine getirirken yönetim kurulu tarafından desteklenir. Yasal olarak bir veri koruma görevlisi atamaktan sorumlu olan grup şirketleri genelde veri koruma için grup yetkilisini atamaktadır. Veri koruma için grup yetkilisi doğrudan Mercedes-Benz Group AG'nin yönetim kuruluna ve veri koruma için grup yetkilisinin atandığı tüm grup şirketlerinin genel müdürüne rapor vermektedir. Özel istisnai durumlarda veri koruma için grup yetkilileri ile mutabakat sağlanmalıdır.

Mercedes-Benz Group AG'nin denetim kurulu mevcut raporlama yükümlülükleri kapsamında veri koruma için grup yetkilisinin yıllık raporu hakkında bilgilendirilmelidir.

İlgili her kişi veri koruması ile ilgili sorunlarını paylaşmak, sorular sormak, bilgi talep etmek veya şikayette bulunmak veya veri güvenliği sorunlarını iletmek için her zaman veri koruma için grup yetkilisine başvurabilir. İstek üzerine soru ve şikayetler gizli tutulur.

Veri koruma için grup yetkilisinin iletişim bilgileri şu şekildedir:

Mercedes-Benz Group AG, veri koruma için grup yetkilisi, HPC E600, 70546 Stuttgart, Germany
E-posta: *data.protection@mercedes-benz.com*
Intranet: *https://social.intra.corpintra.net/docs/DOC-71499*

Mercedes-Benz Group ayrıca özel dahili kurallar ile ayrıntılı açıklanmış olan bir Compliance organizasyonu kurmuştur. Compliance organizasyonu veri korumaya ilişkin talimatlara uyulması konusunda grup şirketlerini destekler ve kontrol eder. İçerik olarak veri koruma eğitimlerini tasarlar ve katılımcı çevresi için kriterleri belirler.

Compliance organizasyonu:
- veri korumasına uyulması konusunda grup şirketlerini destekler ve kontrol eder
- veri koruma eğitimlerini tasarlar.

13.4 Yaptırımlar

Kişisel verilerin uygunsuz bir şekilde işlenmesi veya veri koruma yasalarına yönelik başka ihlaller birçok ülkede kovuşturmalara ve ayrıca tazminat taleplerine yol açabilir. Münferit çalışanların sorumlu olduğu ihlaller iş kanunu ile ilgili yaptırımlara neden olabilir. Bu yönetmeliğin ihlalleri dahili düzenlemelere göre cezalandırılacaktır.

Veri koruma ihlalleri, tazminat taleplerine ve iş kanunu önlemlerine yol açabilir.

13.5 Denetim ve kontroller

Bu yönetmeliğe ve geçerli veri koruma yasalarına uyulduğu grup düzeyinde düzenli olarak yılda en az bir kez risk bazlı olarak kontrol edilmektedir. Bu, dahili bir Compliance risk değerlendirmesi, özel veri koruma konularını içeren denetimler ve diğer kontroller yardımıyla gerçekleştirilir. Veri koruma için grup yetkilisi başka kontrol talebinde bulunma hakkına sahiptir. Sonuçlar veri koruması için grup yetkilisine, sorumlu grup şirketine ve atanmış olması durumunda veri koruma görevlisine iletilmelidir.

Mercedes-Benz Group AG yönetim kurulu mevcut raporlama yükümlülükleri kapsamında sonuçlar hakkında bilgilendirilmelidir. Kontrollerin sonuçları talep üzerine sorumlu veri koruma denetim makamına sunulur. Sorumlu veri koruma denetim makamı DSGVO ve devlet yasalarına göre sahip olduğu yetkiler kapsamında grup şirketlerini bu yönetmeliğin talimatlarına uyulup uyulmadığına dair bir veri koruma denetimine tabi tutabilir.

14 Yönetmelik değişiklikleri ve makamlarla iş birliği

14.1 Değişiklik durumunda sorumluluklar

Bu yönetmelik, veri koruması için grup yetkilisi ile birlikte yönetmeliklerin değiştirilmesine yönelik tanımlanan yöntem kapsamında (*Yönetmelik yönetimi ile ilgili yönetmelik, A 1)* değiştirilebilir. Bu yönetmeliği önemli ölçüde etkileyen veya sağlanan koruma seviyesini muhtemelen etkileyen değişiklikler (yani bağlayıcı nitelikteki değişiklikler) bu yönetmeliğin bağlayıcı kurumsal kurallar olarak onaylanmasını sağlayacak olan ilgili denetim makamlarına gecikmeksizin bildirilecektir.

Bu kılavuzdaki değişiklikler veri koruması için grup yetkilisi ile kararlaştırılmalıdır.

Grup temsilcisi, bu yönetmelik ile bağlı olan tüm grup şirketlerinin güncel bir listesini tutacak (aynı zamanda geçerli düzenleme "*AB veri koruma yönetmeliğine tabi grup şirketlerinin listesi*") ve bu yönetmelikteki her türlü güncellemeyi takip edip kaydedecek ve talep üzerine ilgili kişilere veya denetim makamlarına gerekli bilgileri sağlayacaktır. Bu yönetmelik temelinde kişisel veriler, yeni grup şirketi etkili bir şekilde bu yönetmeliğe bağlı hale gelene ve yönetmeliğe uyulmasına yönelik ilgili Compliance tedbirlerini dikkate alana kadar yeni bir grup şirketine aktarılmaz.

İlgili kişi bu yönetmeliğe erişme hakkına sahiptir. Bu nedenle bu yönetmeliğin en yeni versiyonu internette *https://www.group.mercedes-benz.com* adresinde veri koruma altında yayınlanmıştır. Bu talimat ilgili kişi için üçüncü taraf lehinedir.

Bu yönetmelikte veya bağlı olan grup şirketleri listesinde bir değişiklik yapıldığı takdirde Mercedes-Benz Group AG'nin ana şubesinin denetim makamı, yılda bir kez veri koruması için grup yetkilisi tarafından bunun hakkında bilgilendirilir. Bu durumda güncellemenin nedenleri kısaca açıklanmalıdır.

14.2 Makamlarla iş birliği

Üçüncü ülkelerde işlemeler gerçekleştiren veya buna katılan grup şirketleri, yukarıda belirtilen bağlamda kişisel verilerin işlemesi ile ilgili sorunlar, talepler veya başka işlemler söz konusu olduğunda denetim makamı ile birlikte çalışmakla yükümlüdür. Bu, DSGVO'nun ve ulusal yasalarınızın izin verdiği ölçüde denetim makamlarının denetimlerini kabul etme yükümlülüğünü içerir. Bunun dışında denetim makamının üçüncü ülkelerdeki veri işleme prosesleri veya bu yönetmeliğin düzenlemeleri nedeniyle verdiği DSGVO'ya uygun tüm talimatlara uyulmalıdır.

Yetkili makamlarla iş birliği yapma yükümlülüğü şunları içermektedir:
- denetimlerin kabul edilmesi
- talimatlara uyulması.

Makamlarla iş birliği ile ilgili Madde 14.2 düzenlemeleri ilgili kişi için üçüncü taraf lehinedir.

15 Kişisel verilerin AB/AEA'dan üçüncü bir ülkeye aktarılması

15.1 Verilerin Mercedes-Benz Group dışına aktarılması

Grup şirketleri, kişisel verileri AB/AEA'dan AB/AEA dışındaki üçüncü taraflara (üçüncü bir ülkeden erişim dahil) yalnızca aşağıdaki durumlarda aktarabilir:

- üçüncü taraf ülke, AB Komisyonu tarafından tanınan yeterli veri koruması seviyesi sunuyorsa veya
- aktarım, AB standart sözleşme maddelerine tabiyse. AB standart sözleşme maddelerinin sağladığı garantilerin uygulamada karşılanıp karşılanamayacağına karar vermek için AB yasalarının gerektirdiği koruma düzeyine üçüncü ülkede uyulup uyulmadığını, gerekirse üçüncü tarafın da yardımıyla değerlendirmek grup şirketinin sorumluluğundadır. Böyle bir durum söz konusu değilse,

üçüncü taraf AB/AEA'da öngörüldüğü şekilde büyük ölçüde eşdeğer bir koruma düzeyi sağlamak için tamamlayıcı tedbirler almalıdır, veya

- DSGVO Madde 46 paragraf 2 kapsamındaki diğer uygun garantiler mevcutsa, veya
- istisnai olarak (yani sadece yukarıdaki önlemler uygulanamıyorsa), belirli durumlarda bir istisna uygulanıyorsa (örneğin, yasal hakların talep edilmesi, uygulanması veya savunulması için verilerin aktarılması gereklidir).

15.2 Verilerin Mercedes-Benz Group içine aktarılması

Grup şirketleri, kişisel verileri AB/AEA dışındaki bir grup şirketine aktarmadan önce, üçüncü ülkedeki yasal hükümlerin ve uygulamaların bu yönetmelik kapsamındaki yükümlülüklerini yerine getirmelerini engelleyip engellemediğini kontrol etmelidir. Gerekirse, üçüncü taraf ülkedeki grup şirketi, AB/AEA'da sağlanan korumaya büyük ölçüde eşdeğer bir koruma seviyesi sağlamak için ek sözleşmesel, teknik veya organizasyonel güvenceler uygulamalıdır.

Aktarımın özel koşulları (özellikle veri kategorileri, aktarım türü, üçüncü bir tarafa aktarım) ve verilerin yetkili makamlara ifşa edilmesini gerektiren veya yetkili makamların bu verilere erişimine izin verenler de dahil olmak üzere üçüncü ülkedeki grup şirketi için geçerli olan yasal hükümler ve uygulamalar dikkate alınacaktır.

Grup şirketleri Madde 15.1 ve 15.2'ye ilişkin değerlendirmeyi belgelendirir ve talep üzerine bunları yetkili denetim makamının kullanımına sunar. Ayrıca, grup şirketleri değerlendirmeyi ve sonuçları, diğer grup şirketleri tarafından yapılan aynı tür aktarımlar için belirlenen tamamlayıcı önlemlerin uygulanabilmesi veya etkili tamamlayıcı önlemler alınamazsa aktarımın askıya alınması veya sonlandırılması amacıyla diğer tüm grup şirketleri için şeffaf hale getirir. Bu değerlendirmenin gerçekleştirilmesi için Mercedes-Benz Group AG tarafından sağlanan talimatlara (örneğin araçlar, değerlendirmenin gerçekleştirilmesi için talimatlar) uyulmalıdır.

16 Üçüncü ülke düzenlemelerinin denetimi ve raporlanması

Üçüncü taraf ülkelerdeki grup şirketleri, kendileri için geçerli olan mevzuatın grup şirketlerinin bu yönetmelik kapsamındaki yükümlülüklerini yerine getirmelerini engellediğine veya bu yönetmelikte öngörülen güvenceler üzerinde önemli bir etkiye sahip olduğuna inanmaları için bir neden varsa, veri korumasından sorumlu şirketler grubu yetkilisini bilgilendirmelidir.
Üçüncü taraf ülkelerdeki grup şirketleri, kendileri için geçerli olan mevzuatın grup şirketlerinin bu yönetmelik kapsamındaki yükümlülüklerini yerine getirmelerini engellediğine veya bu yönetmelikte öngörülen güvenceler üzerinde önemli bir etkiye sahip olduğuna

inanmaları için bir neden varsa, veri korumasından sorumlu şirketler grubu yetkilisini gecikmeksizin haberdar etmelidir.

Veri koruma için grup yetkilisi etkiyi değerlendirecek ve bu yönetmeliğin amacını karşılayan pratik bir çözüm bulmak için sorumlu grup şirketiyle birlikte çalışacaktır. Bu değerlendirmeden sonra dahi ilgili yasal gerekliliğin bu yönetmelikte öngörülen güvenceler üzerinde önemli bir olumsuz etkiye sahip olduğu düşünülürse Veri koruma için grup yetkilisi yetkili denetim makamını bilgilendirecektir. Bu tür gerekliliklerin bu yönetmelikte öngörülen güvenceler üzerinde önemli bir olumsuz etkisi olması halinde, bir kolluk kuvveti veya devlet güvenlik makamı tarafından kişisel verilerin ifşa edilmesine yönelik yasal olarak bağlayıcı talepler de buna dahildir. Denetim makamı talep edilen veriler, talep eden makam ve ifşanın yasal dayanağı (aksi yasaklanmadıkça) hakkında bilgilendirilmelidir.

Bir üçüncü ülke grup şirketi bir makam tarafından kişisel verilerin veri koruma denetimine ifşasına yönelik bilgileri vermemekle yükümlü olduğunda bu yasağı mümkün olduğunca hafifletmek veya kaldırmak ve veri koruma denetimine bu eylem alanı içerisinde her yıl alınan başvurular hakkında genel bilgiler sunmak için uygun tedbirler alır (örneğin ifşa başvurularının sayısı, başvurulan verilerin türü, mümkün olduğunca başvuruda bulunan yer).

Kişisel veriler bir kuruma yalnızca toplu, orantısız veya ayrımlaştırılmamış olmadıkları ve bu bağlamda demokratik bir toplumda gerekli olarak görülen sınırları aşmadıkları sürece aktarılabilir.

Bu düzenleme ilgili kişi için üçüncü taraf lehinedir.

Mercedes-Benz Group AG, Mercedesstraße 120, 70327 Stuttgart, Germany, www.group.mercedes-benz.com