

# AB Veri Koruması Politikası



# İçindekiler

<b>1</b>	<b>Yönetmeliğin hedefi</b>	<b>4</b>
<b>2</b>	<b>Uygulama alanı</b>	<b>4</b>
<b>3</b>	<b>Mercedes-Benz Group içerisinde yasal bağlayıcılık</b>	<b>5</b>
<b>4</b>	<b>Yasal gereksinimlere istinaden</b>	<b>5</b>
<b>5</b>	<b>Kişisel verilerin işlenmesi ile ilgili genel temel kurallar</b>	<b>5</b>
5.1	Yasallık	5
5.2	Müşteri ve ortak verilerinin yasal dayanağı	6
5.2.1	Sözleşmesel bir ilişki için veri işleme	6
5.2.2	Reklam amaçlı veri işleme	6
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	7
5.4	Özellikle korunması gereken verilerin işlenmesi	8
5.5	Otomatikleştirilmiş münferit durum kararları (varsa Profiling dahil)	8
5.6	Bilgi verme yükümlülüğü/şeffaflık	8
5.7	Amaca uygunluk	8
5.8	Verilerin minimizasyonu	9
5.9	Verilerin doğruluğu	9
5.10	Privacy by Design & Privacy by Default	9
5.11	Silme ve anonimleştirme	9
5.12	Verilerin işlenmesinde güvenlik	10
5.13	Verilerin Mercedes-Benz Group dışına (iletilmesi) aktarılması	10
<b>6</b>	<b>Veri koruma sonuçlarının değerlendirilmesi</b>	<b>11</b>
<b>7</b>	<b>Veri işleme yöntemlerinin dokümantasyonu</b>	<b>11</b>
<b>8</b>	<b>İş emri üzerine işleme</b>	<b>11</b>
8.1	Genel hususlar	11
8.2	Görevlendiren için düzenlemeler	12
8.3	Görevlendirilenler ile ilgili grup içerisindeki düzenlemeler	12

<b>9 Ortak sorumluluk</b>	<b>13</b>
<b>10 İlgili kişiler için uygulanabilir haklar</b>	<b>13</b>
10.1 İlgili kişinin hakları	13
10.2 Şikayet yöntemi	14
<b>11 Sorumluluk ve yetkili mahkeme</b>	<b>15</b>
11.1 Sorumluluk düzenlemeleri	15
11.2 Yetkili mahkeme	15
<b>12 Veri koruma vakalarının bildirilmesi</b>	<b>15</b>
<b>13 Veri koruma organizasyonu ve yaptırımlar</b>	<b>16</b>
13.1 Sorumluluk	16
13.2 Farkındalık oluşturma ve eğitim	16
13.3 Organizasyon	16
13.4 Yaptırımlar	17
13.5 Denetim ve kontroller	17
<b>14 Yönetmelik değişiklikleri ve makamlarla iş birliği</b>	<b>17</b>
14.1 Değişiklik durumunda sorumluluklar	17
14.2 Makamlarla iş birliği	18
14.3 Üçüncü ülke düzenlemelerinin denetimi ve raporlanması	18

# 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 aktarılabilmesi 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 – BCR") 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<sup>1</sup> için de geçerlidir. Yönetmelik kişisel verilerin işlenmesi 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.

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

<sup>1</sup> Bu yönetmelikte salt dilin basitleştirilmesi amacıyla sadece eril hitap şekli kullanılacaktır. İçerik olarak her durumda tüm cinsel kimlikler kastedilmektedir.

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. Bu yönetmeliğe uyulması ulusal yasanın ihlal edilmesine neden olacaksa ilgili talimatlar ve yasalar önceliklidir. Bu yönetmeliğin içeriği ilgili ulusal yasalar olmadığında da dikkate alınmalıdır.

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

#### Yasalılık

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 işlenmesine 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 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.

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

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 işleminin tür ve kapsamı yasal olarak izin verilen veri işleme için gerekli olmalı ve bu yasalara uygun yapılmalıdır.

### 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 ekonomik (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.

### 5.3 5.3.1

#### **Çalışan verileri için yasal dayanak 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.

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 işlenmesi 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.

### 5.3.4

#### **Veri işleme için muvafakat**

Çalışan verilerinin işlenmesi ilgili kişinin onayı doğrultusunda gerçekleşebilir. Onay beyanmaları 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.

İş ilişkisinin gerçekleştirilmesi dışında (örn. performans kontrolü) çalışanlara ait verilerin işlenmesini gerektiren kontrol önlemleri yalnızca yasal bir zorunluluk bulunduğu ya da açık bir sebep bulunduğu 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), önlemleri 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 işlenmesi 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 yükümlülüklerle uymak için izin verilebilir.

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 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. Veriler DSGVO'nun geçerlilik alanı içerisinde değilse, bilgiler geçerli ulusal yasalara uygun olarak sağlanır. Bilgilendirme net, şeffaf, anlaşılır ve kolay erişilebilir bir şekilde ve sade ve kolay bir dil ile gerçekleştirilmelidir. Veri korumasından sorumlu 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.

#### 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.



### 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.

### 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 alınmalıdır.

### 5.10 Privacy by Design & Privacy by Default

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

Kişisel veriler, yetkisiz erişime ve yasa dışı işleme 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 Verilerin Mercedes-Benz Group dışına (iletilmesi) aktarılması

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.

Kişisel verilerin ülke sınırları dışına aktarılması durumunda (başka bir ülkede erişim sağlanması dahi) kişisel verilerin yurt dışına aktarılması için geçerli ulusal gereksinimler karşılanmış olmalıdır. AB/AEB ülkelerinden kişisel veriler grup şirketleri dışında bulunan üçüncü bir ülkede yalnızca alıcı, bu yönetmeliğe uygun olan bir veri koruma standardına sahip olduğunu kanıtladığı takdirde işlenebilir. Uygun standartlar arasında yer alanlar:

- AB standart sözleşme maddesi ile ilgili anlaşma,
- Alıcının yeterli bir veri koruma seviyesi sağlamak için AB tarafından akredite edilmiş bir sertifikalandırma sistemine katılması veya
- Sorumlu veri koruma denetimi ile uygun bir veri koruma seviyesinin oluşturulması için alıcının bağlayıcı olan şirket kurallarının tanınması.

Kişisel veriler bir kuruma yalnızca toplu, orantısız veya ayrımlaştırılmamış olmadıkları ve bu bağlamda demokratik bir toplumda gerekli olarak görülen sınırları aşmadıkları sürece aktarılabilir. Söz konusu talimatlar ve kuruma ait talimatlar arasında uyumsuzluk olması durumunda Mercedes-Benz Group AG bu yönetmeliğin amacına (Madde 14.3) uygun olan pratik bir çözüm bulmak için ilgili grup şirketi ile birlikte çalışacaktır.

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 gerçekleştirilmektedir (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 korumadan sorumlu 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 gerçekleştirilmesine yönelik talimatlar) dikkate alınmalıdır.

## 7 Veri işleme yöntemlerinin dokümantasyonu

Her bir grup şirketi kişisel verilerin işlendiği yöntemleri bir yöntem kaydında dokümente 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.

## 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 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 belirtilen talimatlara uyulmalı ancak görevlendiren uzmanlık bölümü bunların uygulandığından emin olmalıdır:

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

## 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 korumasından sorumlu grup görevlisinin talimatları dikkate alınmalıdır.
- Verilerin hangi şekilde işlendiğine ve hangi haklara sahip olduğuna 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. Ancak grup şirketinin işleme için zorlayıcı nedenleri varsa veya işleme, yasal hakları kullanmak, uygulamak veya savunmak için gerçekleştirildiğinde, itiraz hakkı mevcut değildir. Haklı bir itiraz durumunda veriler silinmelidir.

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 korumasından sorumlu grup yetkilisine bir şikayette bulunma hakkına sahiptir. Bu tarz şikayetler e-posta üzerinden gönderilebilir.

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.

İlgili kişinin, grup şirketinin talimatlara uyulmasına dair kararı ile aynı fikirde olmaması durumunda (veya başka nedenlerden dolayı konuyu ele alma şekline memnun olmaması durumunda) ilgili kişi bu karara veya bu davranışa karşı haklarını kullanarak temyize başvurabilir. Bunun için özellikle mutad 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.

# 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 ihalden 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 mutad meskenindeki mahkemelerde dava açabilir.

Verilerin bir üçüncü ülkede işlenmesi kapsamında bu yönetmeliğe karşı bir ihalden 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 mutad 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. Gerçek kişilerin hakları ve özgürlükleri için olası bir risk oluşması durumunda ilgili olaylar, grup şirketi ihlali öğrendikten sonra mümkünse 72 saat içerisinde sorumlu denetim makamına bildirilmelidir. 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.

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

Her bir veri koruma ihlali dokümanite 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. 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 süreçlerin geliştirilmesine katıldıkları sürece bu yönetmeliğin içeriği ve ele alınması dahil olmak üzere tüm çalışanların gerekli veri koruma eğitimlerini almasını ve bunlara katılmasını sağlamalıdır. Veri korumasından sorumlu grup yetkilisinin ve Data Compliance'ın talimatları dikkate alınmalıdır.

## 13.3 Organizasyon

Veri koruması 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 koruması için grup yetkilisi ile mutabakata varmalıdır.

Veri koruması 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 koruması için grup yetkilisini atamaktadır. Veri koruması için grup yetkilisi doğrudan Mercedes-Benz Group AG'nin yönetim kuruluna ve veri koruması için grup yetkilisinin atandığı tüm grup şirketlerinin genel müdürüne rapor vermektedir. Özel istisnai durumlarda grubun sorumlu makamları ile veri gizliliği için mutabakat sağlanmalıdır.

Mercedes-Benz Group AG'nin denetim kurulu mevcut raporlama yükümlülükleri kapsamında veri koruması 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 koruması için grup yetkilisine başvurabilir. İstek üzerine soru ve şikayetler gizli tutulur.

Veri koruması için grup yetkilisinin iletişim bilgileri şu şekildedir:

Mercedes-Benz Group AG, veri koruması için grup yetkilisi, HPC E600,  
70546 Stuttgart, Germany

E-posta: [data.protection@mercedes-benz.com](mailto: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.



#### 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.

#### 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 koruması 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 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. Veri koruma yönetmeliği AB, A 17'yi önemli ölçüde etkileyen veya sağlanan koruma seviyesini muhtemelen etkileyen değişiklikler (yani bağlayıcılık değişiklikleri) derhal bu yönetmelik onayını bağlayıcı şirket kuralı olarak veren ilgili veri koruma makamına bildirilmelidir.

Veri koruması için grup yetkilisi bu yönetmeliğe bağlı olan tüm grup şirketlerinin bulunduğu güncel bir liste yapmaktan sorumludur (aynı zamanda geçerli düzenleme "AB veri koruma yönetmeliğine bağlı grup şirketlerinin listesi"). 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 güncellenmenin nedenleri kısaca açıklanmalıdır.

## 14.2

### Makamlarla iş birliği

Üçüncü ülkelerde işlemler gerçekleştiren veya buna katılan grup şirketleri, yukarıda belirtilen bağlamda kişisel verilerin işlenmesi ile ilgili sorunlar, talepler veya başka işlemler söz konusu olduğunda ilgili denetim makamı ile birlikte çalışmakla yükümlüdür. Buna denetim makamları tarafından düzenli denetimleri kabul etme yükümlülüğü dahildir. Bunun dışında sorumlu denetim makamının üçüncü ülkelerdeki veri işleme prosesleri veya bu yönetmeliğin düzenlemeleri nedeniyle verdiği yasalara uygun tüm talimatlara uyulmalıdır.

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

## 14.3

### Üçüncü ülke düzenlemelerinin denetimi ve raporlanması

Üçüncü ülke şirketlerindeki sorumlular, şirketleri için bir kurum veya üye devletlerden biri olarak AB tarafından çıkarılmamış yasaların veya diğer düzenlemelerin aşağıdaki riskleri içerdiğine dair meşru bir varsayım varsa, veri koruması için grup yetkilisini derhal bilgilendirmelidir:

- ilgili üçüncü ülke şirketinin veya başka bir grup şirketinin üçüncü ülkelerde işleme bağlamında bu yönetmelik kapsamındaki yükümlülüklerini yerine getirmesini önlemeye yönelik yasa veya diğer düzenlemelerin uygun olması halinde veya
- yasaların veya diğer düzenlemelerin üçüncü ülkelerde işlenirken bu yönetmelik kapsamında ilgili kişilere tanınan haklar üzerinde önemli bir olumsuz etkisi olması durumunda. Bu, özellikle yerel makamlar, demokratik bir toplumda gerekli olduğu düşünülen sınırları aşan, kitlesel, orantısız veya farklılaşmamış bir kişisel veri aktarımı gerektiriyorsa geçerlidir.

Veri koruması için grup yetkilisi, etkileri değerlendirir ve varsa ilgili yasal gerekliliğin yönetmelik tarafından sağlanan garantileri önemli ölçüde bozma olasılığı varsa, sorumlu veri koruma denetim makamını bilgilendirir. Bu düzenleme ilgili kişi için üçüncü taraf lehinedir.

Bir üçüncü ülke 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, başvuru alan verilerin türü, mümkün olduğunca başvuruda bulunan yer).

