Veri İşleyen Olarak Bağlayıcı Şirket Kuralları

|  |
| --- |
| Bağlayıcı Şirket Kuralları Veri Sorumlusu dokümanı, Avrupa Lider Kuruluşu olarak hareket eden Webhelp SAS çatısı altında bulunan Concentrix iştiraki için geçerlidir.  Bağlayıcı Şirket Kurallarının uygulandığı İştirakler, BCR Ek 01’de listelenmiştir. |

İçindekiler

[1. Giriş 3](#_Toc177054474)

[2. Kapsam 4](#_Toc177054475)

[2.1 Maddi kapsam 4](#_Toc177054476)

[2.2 Coğrafi kapsam 5](#_Toc177054477)

[3. Bağlayıcı Mahiyet 5](#_Toc177054478)

[3.1 Concentrix çalışanları üzerinde 5](#_Toc177054479)

[3.2 Concentrix Grubunun BCR Üyeleri üzerinde 5](#_Toc177054480)

[3.3 Concentrix Veri İşleyenlerine karşı 6](#_Toc177054481)

[4. Kişisel verilerin işlenmesine ilişkin ilkeler 7](#_Toc177054482)

[4.1 Şeffaflık, adalet ve yasaya uygunluk 7](#_Toc177054483)

[4.2 Amaç sınırlaması 8](#_Toc177054484)

[4.3 Veri kalitesi 8](#_Toc177054485)

[4.4 Veri işleme faaliyetlerinin kaydı 9](#_Toc177054486)

[4.5 Güvenlik 9](#_Toc177054487)

[4.6 İlgili Kişilerin Hakları 9](#_Toc177054488)

[4.7 Alt Veri İşleme ve ileriye dönük veri aktarımları 10](#_Toc177054489)

[5. Hassas verilerin işlenmesi 11](#_Toc177054490)

[6. Kişisel Verilerin üçüncü ülkelere aktarılması ve BCR Üyesi Olmayanlara İleriye Dönük Aktarım kısıtlaması 11](#_Toc177054491)

[6.1 Kişisel Veri Aktarımları ve ileriye dönük Aktarımlar 11](#_Toc177054492)

[6.2 Devletin erişim talebi durumunda Veri Alıcısının yükümlülüğü 12](#_Toc177054493)

[7. İlgili Kişinin Hakları 13](#_Toc177054494)

[7.1 Üçüncü Taraf Lehtar Hakları 14](#_Toc177054495)

[7.2 AEA dışındaki bir BCR Üyesinin BCR-P’ye uymaması durumunda şikayette bulunma ve yargısal çözüm, düzeltme ve tazminat alma hakkı 16](#_Toc177054496)

[7.3 İlgili Kişilerin Hakları 16](#_Toc177054497)

[7.4 İlgili Kişilerin Haklarının Kullanılması 17](#_Toc177054498)

[8. İlgili Kişilerin şikayet yönetimi prosedürü 18](#_Toc177054499)

[9. Harici Müşterilerin Şikayetleri 19](#_Toc177054500)

[10. Veri koruma yönetimi 19](#_Toc177054501)

[11. Eğitim ve farkındalık 20](#_Toc177054502)

[12. Kasten gizlilik/varsayılan gizlilik 21](#_Toc177054503)

[13. Şeffaflık ve iş birliği 21](#_Toc177054504)

[13.1 BCR-P İletişimi 21](#_Toc177054505)

[13.2 İlgili Kişilere Sağlanan Bilgiler 22](#_Toc177054506)

[13.3 BCR-P’ye uyumu etkileyen yerel mevzuat ve uygulamalarla tutarsızlıklar 22](#_Toc177054507)

[13.4 İş birliği yapma görevi 24](#_Toc177054508)

[14. BCR’yi kapsayan denetim programı 25](#_Toc177054509)

[15. BCR-P’de değişiklik 27](#_Toc177054510)

[16. BCR-P’ye uyulmaması 28](#_Toc177054511)

[17. Fesih 28](#_Toc177054512)

[18. Ekler 29](#_Toc177054513)

[BELGE KONTROLÜ 30](#_Toc177054514)

1. Giriş

|  |
| --- |
| **Hatırlatıcı:** **Eylül 2023 tarihinde gerçekleşen Webhelp & Concentrix işleminin ardından, grubun ticari adı artık Concentrix olarak belirlenmiştir. Bununla birlikte, mevcut Bağlayıcı Şirket Kuralları (BCR) kapsamının değiştirilmediğini lütfen unutmayınız. Bağlayıcı Şirket Kuralları yalnızca Avrupa Lider Kuruluşu olarak hareket eden Webhelp SAS çatısı altındaki İştirakler için geçerlidir. Bağlayıcı Şirket Kurallarına (Veri Sorumlusu ve/veya Veri İşleyen) tabi olan İştirakler, Ek 01’de listelenmiş olup BCR Üyesi olarak anılacaktır.** |

Concentrix Grubu olarak, Kişisel Verilerin korunmasının yalnızca bir güvenlik veya belirli bir yasal çerçeveye uyum meselesi olmadığına, daha ziyade bireysel ve kurumsal bir taahhüt meselesi olduğuna inanıyoruz. Concentrix standartlarının işbu Veri İşleyenler için Bağlayıcı Şirket Kuralları (bundan böyle “BCR-P”) ve Veri Sorumluları için Bağlayıcı Şirket Kuralları (bundan böyle “BCR-C”) vasıtasıyla açıklanması ve paylaşılması, İlgili Kişilerin Kişisel Verilerinin nasıl İşlendiğine ilişkin meşru beklentileri açısından son derece önemlidir.

BCR Üyeleri faaliyetleri sırasında hem kurum içi verileri hem de Müşterinin Kişisel Verilerini işlerler. Bu bağlamda, BCR Üyeleri Müşterileri adına işlediği Kişisel Verileri işbu BCR-P dokümanında yer alan uygun teknik, fiziki ve idari önlem ve kontrollerin uygulanması suretiyle korurlar. Söz konusu kontroller, tüm kuruluşun Veri İşlemenin niteliğini ve/veya yerini dikkate almadan Kişisel Verileri tutarlı bir şekilde İşlemesini sağlayacaktır.

Bu yaklaşım, Concentrix’in Müşterileri adına ele aldığı faaliyetlerin çeşitliliği nedeniyle özellikle önemlidir.

Yukarıdaki hususların bir sonucu olarak ve 27 Nisan 2016 tarihinde kabul edilen 2016/679 sayılı Avrupa Birliği Genel Veri Koruma Tüzüğü (bundan böyle “**AB Tüzüğü**” veya “**GDPR**”) ile getirilen gerekliliklerin yanı sıra AB Tüzüğü ile çelişmediği takdirde veri koruma alanında yürürlükte olan standart, yönetmelik ve yasaları dikkate alarak, BCR Üyeleri Kişisel Verileri aşağıdaki ilkeler doğrultusunda İşleyecektir:

* **Yasaya Uygunluk** – Kişisel Veriler, İlgili Kişi tarafından Veri İşlemeye onay verildiği takdirde veya söz konusu Veri İşleme Yürürlükteki Veri Koruma Mevzuatı uyarınca meşru veya gerekli olduğunda toplanacak ve İşlenecektir.
* **Adalet** – Kişisel Verilerin İşlenmesinde söz konusu Kişisel Verilerin İşlendiği özel koşullar ve bağlam dikkate alınacaktır.
* **Şeffaflık** – Kişisel Verilerin İşlenmesine ilişkin bilgi ve iletişim kolay erişilebilir, kolay anlaşılır, net, açık ve sade bir dille olmalıdır.
* **Amaç sınırlaması** – Kişisel Veriler belirli, açık ve meşru amaçlar için toplanacak olup bu amaçlarla bağdaşmayan bir şekilde daha fazla İşlenmeyecektir.
* **Verilerin asgariye indirilmesi** – Toplanan Kişisel Veriler, İşlendikleri amaçlar doğrultusunda yeterli, alakalı ve gerekli olanlarla sınırlı olacaktır.
* **Doğruluk** – Kişisel Veriler doğru olacak ve gerektiğinde güncel tutulacaktır. Veri işleme amaçları göz önüne alındığında, doğru olmayan Kişisel Verilerin fazla gecikmeden silinmesini veya düzeltilmesini sağlayacak her makul adım atılmalıdır.
* **Saklama sınırlaması** – Kişisel Veriler, söz konusu verilerin İşlenme amaçları veya diğer yasal saklama süreleri için gerekenden daha uzun süre İlgili Kişilerin kimlik tespitine olanak tanıyan bir biçimde tutulmayacaktır.
* **Bütünlük ve gizlilik** – Kişisel Veriler uygun teknik, fiziki ve idari önlemlerin uygulanması suretiyle yetkisiz veya kanuna aykırı Veri İşleme süreçlerine ve Kişisel Verilerin kazayla kaybedilmesi, imha edilmesi veya zarar görmesi gibi durumlara karşı koruma da dahil olmak üzere Kişisel Verilerin güvenliğini sağlayacak şekilde işlenecektir.

Concentrix, işbu BCR-P dokümanı vasıtasıyla tüm BCR Üyeleri için geçerli olan ayrıntı ve ilkeleri paylaşmayı, belirtmeyi ve BCR-C’nin uygulanmasına imkan tanıyan grup çapında belirli standartları sağlamayı amaçlar. Ayrıca Concentrix özel, yerel veya sektörel politikalar da sunabilir. İşbu BCR-P dokümanı ile söz konusu özel, yerel veya sektörel politikalar arasında bir çelişki olması durumunda, bu özel, yerel veya sektörel politikaların çelişkili hükümleri İlgili Kişinin haklarını ve özgürlüğünü daha fazla korumadığı sürece, BCR-P hükümleri esas alınacaktır.

BCR-P, Kişisel Verilerin İşlenmesine ilişkin tüm Concentrix kuruluşu genelinde yeterli ve tutarlı bir yaklaşım sağlamayı amaçladığından, yürürlükteki mevzuatlardan kaynaklanabilecek istisnalar işbu BCR-P dokümanında yansıtılmamıştır. Bununla birlikte, ulusal mevzuatın bir BCR Üyesinin BCR-P’ye uymasını engellediği ve AB Üye Devletlerinin AB Tüzüğüne özel kurallar eklediği durumlarda işbu BCR-P dokümanı, Madde 13.3’de bir bildirim mekanizması içermektedir. Sonuç olarak, yerel mevzuat, işbu BCR-P için yürürlüğe konabilir bir istisna olarak kabul edilecek ve uygun bildirimin ardından buna göre kaydedilecektir. Madde 13.3’te belirtildiği üzere, ulusal mevzuatın Kişisel Veriler için daha yüksek düzeyde bir koruma sağlaması halinde bu ulusal mevzuat, BCR-P’ye göre öncelikli olacaktır.

1. Kapsam
   1. Maddi kapsam

İşbu BCR-P, bir BCR Üyesinin Veri İşleyen olarak Kişisel Verileri İşlediği her durumda geçerlidir.

Concentrix kapsamına giren çok çeşitli faaliyetler ve Concentrix’in Kişisel Verileri esas olarak Müşterileri adına işlemesi nedeniyle, Concentrix aşağıdakiler gibi muhtelif ve sürekli olarak gelişen Kişisel Veri kategorilerini işlemek zorunda kalabilir:

* Özel hayatla ilgili veriler (ör. müşteri memnuniyeti izleme, çevrimiçi sosyal etkileşimlerin yönetimi),
* Ekonomik ve finansal veriler (ör. müşteri ilişkilerinin yönetimi, dolandırıcılığın önlenmesi ve tespiti, faturalama, raporlama ve analizler,
* Kimlik tespiti verileri (ör. gelen ve giden arama yönetimi, çıkış işlemlerinin yönetimi, arama ve etkileşim yönlendirme, dinleme ve kayıt etkileşimleri),
* Teknik veriler (ör. arama ve etkileşim yönlendirme, gelen ve giden işlemler analizi, konuşma analitik çözümü).

Maddi kapsam, işbu BCR-P dokümanı kapsamında ayrıntılı bir Veri İşleme Amaçları ve İlgili Kişi ve Kişisel Veri kategorileri tablosu sunan **Ek 11-B**’de daha kesin olarak detaylandırılmıştır.

Yukarıdakilere bakılmaksızın işbu BCR-P, söz konusu Kişisel Verilerin kategorisinden ve niteliğinden bağımsız olarak Veri İşleyen olarak hareket eden BCR Üyeleri tarafından işlendiği durumları kapsamaktadır.

BCR Üyeleri aynı zamanda işverenleri olarak çalışanlarının Kişisel Verilerinin Veri Sorumlusudur. BCR Üyeleri, Concentrix çalışanlarının Kişisel Verilerini İşlerken BCR-C hükümlerine riayet edecek ve Kişisel Verileri Çalışan Gizlilik Politikasında açıklandığı şekilde işleyecektir.

* 1. Coğrafi kapsam

Concentrix, Kişisel Verilerin işlenmekte olduğu kuruluş bünyesinde mümkün olduğunca tutarlı bir yaklaşım uygulamak istemektedir. Dolayısıyla tüm BCR Üyeleri, konumları veya yasal yargı alanları ne olursa olsun, işbu BCR-P’ye tabidir. Prensip olarak, BCR-P’ye tabi olmadıkça veya tabi olana kadar herhangi bir BCR Üyesi tarafından işbu BCR-P’ye tabi olmayan bir Concentrix kuruluşuna hiçbir Kişisel Veri Aktarımı gerçekleştirilmeyecektir. Söz konusu Concentrix kuruluşu, Veri İşleme ve buna bağlı yükümlülüklerin işbu BCR-P’nin gerekliliklerini karşılayacağı ve İlgili Kişilerin haklarının korunmasını temin edeceği şekilde uygun teknik ve organizasyonel önlemleri uygulamak için yeterli garantiyi sağlamadığı sürece bu tür bir Veri Aktarımı gerçekleştirilemez. BCR-P’ye tabi olan Concentrix Kuruluşu ve tabi olmayan Concentrix kuruluşu, bu durumu garanti etmek için yazılı bir anlaşma yapacaktır.

1. Bağlayıcı Mahiyet
   1. Concentrix çalışanları üzerinde

Kişisel Verilerin korunması bireysel ve kurumsal bir taahhüt meselesi olduğundan, her çalışan işbu BCR-P kapsamında belirtilen gerekliliklere uymalıdır.

Bu nedenle BCR-P, Concentrix çalışanlarının iş sözleşmelerinin bir parçası olarak uymaları gereken politikalar kümesine girer. İşbu BCR-P ilkelerine ve kurallarına uyulmaması, iş akdinin feshiyle sonuçlanabilecek disiplin cezalarına ve belirli durumlarda cezai suçlamalara yol açabilir.

* 1. Concentrix Grubunun BCR Üyeleri üzerinde

Bir grup olarak Concentrix, gruba ait tüm BCR Üyelerinin işbu BCR-P kapsamında belirtilen ilke ve yükümlülüklere aynı veya benzer şekilde tabi olmasını ve burada belirtilen gerekliliklere uymasını sağlamak ister.

Bu nedenle işbu BCR-P, tüm BCR Üyeleri için bu BCR-P dokümanını bir ek olarak içeren Grup İçi Veri Aktarım Sözleşmesinin imzalanmasıyla birlikte bağlayıcıdır.

İşbu BCR-P’ye tabi Concentrix kuruluşları listesi, BCR-P’nin Ek 1’inde belirtilmiştir. Lider Avrupa Kuruluşu olarak Webhelp SAS, Grup Veri Koruma Görevlisinin (DPO) yardımıyla, bu listeyi güncel ve erişilebilir tutmayı ve zaman zaman belirlenen şekilde ilgili taraflara talep üzerine iletmeyi taahhüt eder.

* 1. Concentrix Veri İşleyenlerine karşı

BCR Üyeleri, Müşterisi adına Veri İşleyen olarak hareket ederken işbu BCR-P’ye uymayı ve hem Müşterileri hem de Müşterilerin İlgili Kişileri açısından BCR-P gerekliliklerini uygulamayı taahhüt eder. BCR Üyelerinin, Müşterilerinin İlgili Kişilerinin Kişisel Verilerini İşlediği durumlarda BCR Üyeleri ve Veri İşleme sürecine dahil olan her BCR Üyesi çalışanı, Müşterilerin talimatları doğrultusunda, Bölüm 7 - İlgili Kişilerin Hakları hükmüne tabi olarak söz konusu İlgili Kişinin haklarının korunmasını temin etmeyi ve işlediği Kişisel Verilere yeterli düzeyde koruma sağlamayı taahhüt eder.

Bir BCR Üyesi tarafından bir Müşteri adına gerçekleştirilen Veri İşleme faaliyeti, yazılı bir sözleşme veya diğer bağlayıcı hukuki işlem ile yönetilir ve GDPR Madde 28’in tüm unsurlarını ve özellikle Veri İşlemenin konusunu ve süresini, niteliğini ve amacını, Kişisel Verilerin türünü ve İlgili Kişi kategorilerini ve Veri Sorumlusunun hak ve yükümlülüklerini belirler. Ayrıca bir Veri İşleyen ile yapılan bu sözleşme veya diğer bağlayıcı yasal işlem, aşağıdaki hükümleri düzenleyecektir:

1. Concentrix, özellikle Kişisel Verileri İşlemeye yetkili kişilerin gizliliğe bağlı kalmalarını veya uygun bir yasal gizlilik yükümlülüğü altında olmalarını sağlayarak Kişisel Verileri gizli tutacaktır.
2. Concentrix, Kişisel Verileri korumak için uygun bir güvenlik seviyesi sağlamak üzere uygun teknik, fiziksel ve organizasyonel güvenlik önlemlerini alacaktır.
3. Concentrix, Müşterinin önceden yazılı izni olmadan Müşteriye olan yükümlülüğüyle bağlantılı olarak Alt Veri İşleyenin Kişisel Verileri İşlemesine izin vermeyecek ve bu Alt Veri İşleyenin, Concentrix ile Müşteri arasında Birlik veya Üye Devlet yasaları uyarınca bir sözleşme veya diğer yasal işlem yoluyla akdedilen bağlayıcı işlemde belirtilen aynı yükümlülüklere uymayı taahhüt etmesini sağlayacaktır. Alt Veri İşleyenin veri koruma yükümlülüklerini yerine getirememesi durumunda, ilk Veri İşleyen diğer Veri İşleyen yükümlülüklerinin yerine getirilmesi için BCR Üyesine karşı tam olarak sorumlu olmaya devam edecektir.
4. Concentrix, mevzuata uyum sağladığını göstermek ve Müşteri veya diğer ilgili KURUM tarafından yapılan denetim ve incelemelere katkıda bulunmak için gerekli tüm bilgileri Müşteriye sağlayacaktır.
5. Concentrix, Kişisel Verileri içeren fiili veya şüpheli herhangi bir güvenlik ihlali konusunda Müşteriyi derhal bilgilendirecek ve Müşteriye, duruma göre, ilgili Denetim Kurumuna bildirimde bulunma ve etkilenen İlgili Kişilerle iletişim kurma konusunda destek sağlayacaktır.
6. Concentrix, Müşteriye veri koruma etki değerlendirmesi yapması için tüm makul yardımı sağlayacaktır.
7. Concentrix, İlgili Kişilerin haklarına ilişkin taleplerinin ele alınması konusunda Müşteriye gerekli tüm desteği sağlayacaktır.
8. Concentrix, sözleşmenin veya diğer hukuki bağlayıcı işlemin sona ermesinde Kişisel Verilerin silinmesi veya iadesi ile ilgili Müşterinin talimatlarına uyacaktır.
9. Concentrix, bir talimatın işbu BCR-P’yi veya Geçerli Veri Koruma Mevzuatını ihlal ettiği kanaatine varırsa Müşteriyi derhal bilgilendirecektir.

Söz konusu sözleşme, her iki taraf için de Bağlayıcı Şirket Kurallarını açıklamak ve uygulamak için işbu BCR-P’yi içerecektir. Müşteriler, işbu BCR-P’nin herhangi bir hükmünü bir BCR Üyesine - veya devredilmiş sorumluluğu olan herhangi bir BCR Üyesine - karşı uygulama hakkına sahiptir.

1. Kişisel verilerin işlenmesine ilişkin ilkeler

BCR Üyeleri, Müşterileri adına Veri İşleyen olarak hareket ederken aşağıda tanımlanan ilkelere uyacaktır. Her durumda Müşteri, Kişisel Verilerin kaynağı ne olursa olsun, Geçerli Veri Koruma Mevzuatı ve Concentrix ile Müşteri arasındaki Hizmet Sözleşmesi uyarınca yürütülen tüm Kişisel Veri İşlemelerinden sorumlu olacaktır.

* 1. Şeffaflık, adalet ve yasaya uygunluk

BCR Üyeleri, Veri İşleyen olarak hareket ederken (1) yeterli garantileri sağlamayı ve Veri İşlemenin işbu BCR-P’nin gerekliliklerini karşılayacak şekilde uygun teknik ve organizasyonel önlemleri uygulamayı (2) makul bir süre içinde ve makul surette mümkün olduğu ölçüde Veri Sorumlusu ile iş birliği yapmayı ve Müşterinin Geçerli Veri Koruma Mevzuatına uymasına yardımcı olmayı taahhüt eder. BCR Üyelerinin Müşterisi, Veri Sorumlusu olarak Concentrix’ten talep ettiği Veri İşlemenin gerçekten Geçerli Veri Koruma Mevzuatına uygun olmasını sağlamaktan sorumlu olmaya devam eder.

Veri İşlemenin niteliğini ve mevcut bilgileri dikkate alarak, BCR Üyeleri, Veri İşleme Standardı Ekini tamamlayarak, Müşterinin işlemenin niteliğine, kapsamına, bağlamına ve amaçlarına dayalı olarak bir veri koruma etki değerlendirmesinin gerekli olduğuna inanması halinde Müşteriye yardımcı olacaktır. Müşterinin veri koruma etki değerlendirmesi yapmak, veri koruma kurumlarının soruşturma ve sorgulamalarına yanıt vermek veya Denetim Kurumuna önceden danışmak için ek yardıma ihtiyaç duyması halinde, BCR Üyeleri Veri İşlemenin niteliğini ve kendilerine sunulan bilgileri dikkate alarak Veri Sorumlusu Denetim Programı aracılığıyla Müşteriye yardım sağlayacaktır.

BCR Üyeleri ayrıca Hizmet Sözleşmesinin sona ermesi üzerine, üretim sistemlerinde saklanan Müşterinin Kişisel Verilerinin, AB Yönetmeliğinin 28.3 (g) maddesi uyarınca Concentrix tarafından işlenmesini sağlayacaktır. Herhangi bir Geçerli Veri Koruma Mevzuatı veya başka bir Hizmet Sözleşmesi, Kişisel Verilerin saklanmasını gerektirmediği ve Veri Sorumlusunun yazılı talebine tabi olmadığı sürece, üretim sistemlerinde saklanan Kişisel Veriler, Hizmet Sözleşmesinin sona ermesi üzerine Veri Sorumlusunun tercihi üzerine silinecek veya iade edilecektir. BCR Üyeleri, Veri Sorumlusu ile kararlaştırılan zaman dilimi içinde, Müşteri tarafından aktarılan Kişisel Verilerin gizliliğini garanti etmek ve güvence altına almak ve BCR Üyelerinin aktarılan Kişisel Verileri artık aktif olarak işlemeyeceğini taahhüt etmek zorundadır. Veri Sorumlusu, Kişisel Verilerin silinmesi veya iadesinin (i) kesinlikle Veri Sorumlusu tarafından sağlanan ve talep anında Veri İşleyen olarak hareket eden Concentrix tarafından saklanan Kişisel Verilerle sınırlı olacağını ve (ii) yedekleme depolama gerekliliklerini ve güvenlik politika ve standartlarını dikkate alacağını kabul eder.

Ayrıca bir BCR Üyesinin geçerli mevzuatın kendisinin işbu BCR-P kapsamındaki yükümlülüklerini yerine getirmesini engellediğine veya BCR-P tarafından sağlanan garantiler üzerinde önemli bir etkiye sahip olduğuna inanmak için nedenleri varsa, bu BCR Üyesi Madde **Erreur ! Source du renvoi introuvable.**‘de belirtildiği üzere (geçerli yerel mevzuat veya örneğin bir kolluk kuvveti soruşturmasının gizliliğini korumak için ceza hukuku kapsamında bir yasaklama gibi bir kolluk kuvveti otoritesi tarafından yasaklandığı durumlar hariç olmak üzere) derhal DPO’yu, Webhelp SAS’ı ve diğer ilgili Yerel Gizlilik Liderini ve Müşterileri bilgilendirecektir. Böyle bir durumda Müşteri, veri aktarımını veya eldeki Veri İşleme faaliyetlerini askıya alma ve/veya sözleşmeyi feshetme hakkına sahiptir.

* 1. Amaç sınırlaması

Concentrix, genel bir amaç sınırlaması ilkesine bağlı kalmayı taahhüt eder; buna göre Concentrix, Veri İşleyen olarak hareket ettiği durumlarda Kişisel Verileri Müşterisi adına ve belgelenmiş talimatlarına sıkı sıkıya bağlı kalarak işleyecektir. BCR Üyeleri, bir talimatın Geçerli Veri Koruma Mevzuatını ihlal ettiği kanaatine varırsa Müşteriyi derhal bilgilendirecektir.

Bilhassa BCR Üyeleri, Kişisel Verileri Müşterisi adına şu şekilde işlemeyi taahhüt eder:

* yalnızca söz konusu Müşteri tarafından ifade edilen amaçlar için,
* Concentrix ile Müşterisi arasında Hizmet Sözleşmesi kapsamında kararlaştırılan koşullar altında ve
* BCR Üyesinin Müşterisi tarafından açıkça belirtilen süreden daha uzun olmamak üzere.

Bir BCR Üyesi, söz konusu uygunluğu sağlayamadığı durumda derhal Müşterisini, DPO’yu ve ilgili Yerel Gizlilik Liderini bu konuda bilgilendirmeyi taahhüt eder. Bu tür bilgiler, BCR Üyesi tarafından Müşterisine gecikmeden ve bu tür bir uyumluluğun sağlanamayacağını fark ettiği anda iletilecektir. Böyle bir durumda Müşteri, Kişisel Verilerin BCR Üyesine aktarılmasını veya eldeki Veri İşleme faaliyetlerini askıya alma ve/veya sözleşmeyi feshetme hakkına sahip olacaktır.

* 1. Veri kalitesi

BCR Üyeleri, Geçerli Veri Koruma Mevzuatına uyum konusunda Müşteriye yardımcı ve destek olmayı taahhüt eder.

Özellikle BCR Üyeleri, Kişisel Verilerin güncellenmesi, düzeltilmesi veya silinmesi ya da İlgili Kişinin kullanabileceği diğer herhangi bir hak için Müşterileri tarafından talep edilen gerekli önlemleri uygulamak suretiyle İlgili Kişilerin haklarını kullanmalarını sağlamada Müşterilerine yardımcı olacaktır.

Böyle bir durumda BCR Üyesi, Kişisel Verilerin açıklanmış olduğu her ilgili BCR Üyesini (veya BCR’ye tabi olmayan Concentrix İştirakini) kişisel verilerin düzeltmesi, silinmesi veya anonimleştirilmesi konusunda bilgilendirecektir.

BCR Üyeleri ayrıca Müşterilerinin talebi üzerine ve mümkün olduğunda, söz konusu verilerin tanımlanabilir biçiminin artık gerekli olmadığı andan itibaren Kişisel Verilerin silinmesi veya anonimleştirilmesi için önlemler uygulayacaktır.

* 1. Veri işleme faaliyetlerinin kaydı

BCR Üyeleri, Veri İşleyen olarak hareket ederken bir Veri Sorumlusu adına gerçekleştirilen tüm Kişisel Veri İşleme faaliyeti kategorilerinin kaydını tutacak ve bu kayıtta en azından şunlar yer alacaktır:

1. BCR Üyelerinin ve Concentrix’in adına hareket ettiği Veri Sorumlusunun (Sorumlularının) adı ve iletişim bilgileri,
2. Gerçekleştirilen Veri İşleme kategorileri,
3. Üçüncü bir ülkeye veya uluslararası bir kuruluşa potansiyel Kişisel Veri aktarımları,
4. Veri İşleme riskine uygun bir güvenlik seviyesi sağlamak için gerekli teknik ve organizasyonel güvenlik önlemlerinin genel bir açıklaması.
   1. Güvenlik

BCR Üyeleri, Veri İşleyen olarak hareket ederken en azından Geçerli Veri Koruma Mevzuatının gerekliliklerini ve özellikle GDPR Madde 32 ile Müşteri ile yapılan Hizmet Sözleşmesinde belirtilen mevcut özel önlemleri karşılamak suretiyle Veri İşlemenin taşıdığı risklere uygun bir güvenlik seviyesi sağlamak için tüm uygun teknik ve organizasyonel önlemlere uymayı taahhüt eder.

BCR Üyeleri, bir Kişisel Veri ihlalinin farkına vardıklarında Müşteriyi fazla gecikmeden bilgilendirecek ve Veri Sorumlusu ile iş birliği içinde BCR Üyeleri tarafından uygulanan geçerli Kişisel Veri İhlali prosedürüne uyacaktır.

* 1. İlgili Kişilerin Hakları

BCR Üyeleri, Müşteri tarafından talep edilen gerekli önlemleri almayı ve işbu BCR-P Bölüm 7’de daha ayrıntılı olarak açıklandığı üzere söz konusu Müşterinin İlgili Kişilerin haklarını gözetme görevini yerine getirmesine yardımcı olmak için yararlı bilgileri iletmeyi taahhüt eder.

BCR Üyeleri, veri işlemenin niteliğini ve Veri İşleyenin erişebildiği bilgileri dikkate alarak Müşterinin taleplere yanıt verme yükümlülüğünün yerine getirilmesi için mümkün olduğu ve Müşteri ile kararlaştırıldığı ölçüde Müşteriye yardım ve iş birliği sağlayacaktır. BCR Üyeleri, Veri İşleyen olarak hareket ettikleri durumlarda işbu BCR-P’ye ekli İlgili Kişilerin Taleplerine İlişkin Prosedürü izleyecektir.

Bir BCR Üyesi, İlgili Kişilerden haklarını kullanmak konusunda bir talep aldığında Müşteriyi bu konuda bilgilendirecek ve Müşteri ise talebe yanıt verecektir. Geçerli Veri Koruma Mevzuatı uyarınca Müşteri, bu tür talepleri işleme almaktan sorumludur. BCR Üyesi yalnızca Müşterisinin bu tür taleplerin nasıl ele alınacağına ilişkin diğer Talimatlarına uymaktan ve bu talepleri işleme almak için Müşteriyle iş birliği yapmaktan sorumludur.

* 1. Alt Veri İşleme ve ileriye dönük veri aktarımları

BCR Üyeleri veya üçüncü taraf sağlayıcılar, Müşteri ile kararlaştırılan Hizmet Sözleşmesi hükümlerine uygun olarak Kişisel Verileri Alt Veri İşleyene sağlayabilirler. Alt Veri İşleyenler; Veri İşlemenin Geçerli Veri Koruma Mevzuatı, işbu BCR-P ve yürürlükteki herhangi bir Veri İşleme Sözleşmesinin gerekliliklerini karşılayacağı şekilde uygun teknik ve organizasyonel önlemlerin uygulanması için yeterli garantiyi sağlayacaktır.

BCR Üyeleri, önceden Veri Sorumlusundan yazılı bir izin almadan bir Alt Veri İşleyen kullanmayacaktır. Alt Veri İşleyenlerin kullanılmasına yönelik genel bir izin verildiğinde ilgili BCR Üyesi, Müşteriyi herhangi bir Alt Veri İşleyenin eklenmesi veya değiştirilmesiyle ilgili amaçlanan değişiklikler hakkında bilgilendirerek Müşteriye bu tür değişikliklere itiraz etme ve hem burada hem de Hizmet Sözleşmesi ve Veri İşleme Sözleşmesinde açıklandığı üzere geçerli sipariş formunu (formlarını) feshetme fırsatı verecektir. Yürürlükteki Hizmet Sözleşmesi ve Veri İşleme Sözleşmesi şartlarının ve/veya sipariş formunun (formlarının) Veri Sorumlusunu hizmetlere itiraz etme veya hizmetleri sonlandırma hakkından mahrum etmemesi koşuluyla, Veri Sorumlusu ilgili BCR Üyesine yazılı bildirimde bulunarak itiraz edilen yeni Alt Veri İşleyen kullanımı olmadan BCR Üyesi tarafından sağlanamayan Hizmetlerle ilgili olarak geçerli sipariş formunu (formlarını) feshedebilir.

Alt Veri İşleyen, kendisinin en az Veri Koruma Mevzuatı, işbu BCR-P ve Veri İşleme Sözleşmesinde açıklananlar kadar katı ve en azından eşdeğer koruma düzeyi sunan şart ve yükümlülüklere uymasını gerektiren bir sözleşme veya diğer yasal işlem yoluyla bağlı olacaktır. Müşteri, BCR Üyesinden Kişisel Verileri İşleme yetkisine sahip Alt Veri İşleyenlerin listesini iletmesini makul surette talep edebilir. İlgili sözleşme; Veri İşleme amaçlarını, niteliğini, İşlenen Kişisel Veri kategorileri ile İlgili Kişi kategorilerini açıkça belirtecektir.

Kişisel Verilerin yetkili kurumlara ifşa edilmesi konusunda yasal bir yükümlülük olması durumunda ilgili BCR Üyeleri, bu durumu Webhelp SAS ve DPO’ya bildirmelidir. Webhelp SAS, ilgili AEA Denetim Kurumunu ve aksi yasaklanmadığı sürece Müşteriyi bu ifşa konusunda fazla gecikmeden bilgilendirmeyi ve Verilerin asgariye indirilmesi ilkesine uymayı taahhüt eder. BCR Üyesi söz konusu ifşanın hangi İlgili Kişileri ilgilendirdiğini, hangi kurumun bu ifşayı talep ettiğini ve hangi yasal temele dayandığını açıkça belirtecektir. Her halükarda BCR Üyeleri, Kişisel Verileri resmi kurumlara fazlasıyla ve orantısız bir şekilde aktarmamayı taahhüt eder. Aynı durumda BCR Üyeleri, Müşteriyi ifşa hakkında bilgilendirmeyi taahhüt eder. Bir BCR Üyesine yapılan herhangi bir bildirim ve AEA Denetim Kurumlarına yapılan planlı bildirim, aşağıda Madde 13.3’ün mekanizmasına ve hükümlerine tabidir.

Bunun yanı sıra her BCR Üyesi, tüm Alt Veri İşleyenlerin ve özellikle Kişisel Verilerin İşlenmesine dahil olan diğer BCR Üyelerinin Müşteri tarafından genel veya özel yazılı bir yetkilendirme ile usulüne uygun şekilde onaylanmasını sağlayacak ve bunu doğrulayacaktır.

1. Hassas verilerin işlenmesi

BCR Üyeleri, Madde 4 – Kişisel Verilerin İşlenmesine İlişkin İlkeler hükümlerine uymayı taahhüt eder ve Hassas Kişisel Veriler, İlgili Kişilerin temel hak ve özgürlükleri ile ilgili önemli riskler oluşturabileceğinden Hassas Kişisel Verilerin özel bir koruma uygulanmasını gerektirdiğini kabul eder.

Müşterileri BCR Üyelerinden Hassas Kişisel Verileri İşlemelerini istediğinde, BCR Üyelerinin ek teknik, fiziksel ve idari güvenlik önlemleri ve kontrolleri uygulaması gerekebilir.

Bu konuda hangi önlemlerin uygulanması gerektiğini tanımlamak ve Geçerli Veri Koruma Mevzuatının ve varsa AEA Denetim Kurumları tarafından benimsenen diğer sektörel çerçevenin gerekliliklerinin karşılanmasını sağlamak BCR üyelerinin Müşterisinin sorumluluğunda olacaktır.

Anlaşılabilirlik adına, BCR Üyelerinin Veri İşleyen olarak Hassas Kişisel Verileri İşlediği durumlarda, BCR Üyeleri hiçbir koşulda Veri İşlemenin yukarıda Madde 4 - Kişisel Verilerin İşlenmesine İlişkin İlkeler hükmünde tanımlanan yasal dayanaklardan birine dayanmasını sağlamaktan sorumlu olmayacaktır.

1. Kişisel Verilerin üçüncü ülkelere aktarılması ve BCR Üyesi Olmayanlara İleriye Dönük Aktarım kısıtlaması
   1. Kişisel Veri Aktarımları ve ileriye dönük Aktarımlar

BCR Üyeleri, iş faaliyetleri sırasında Kişisel Verileri Müşterisi veya Müşterileri adına işleyebilir. Söz konusu BCR Üyeleri veya Müşteri(ler), Avrupa Ekonomik Alanı (bundan böyle “AEA”) dışında bulunabilir ve dolayısıyla bu durum Kişisel Verilerin Aktarılmasını gerektirebilir. Böyle bir durumda, işbu BCR-P’nin uygulama kapsamı şudur:

* Veri Sorumlusu olarak hareket eden ve AEA içinde bulunan bir Müşteriden alınan ve daha sonra bu Müşteri adına Veri İşleyen olarak hareket eden BCR Üyeleri tarafından işlenen Kişisel Veriler ve
* Bir Müşteri adına Veri İşleyen olarak hareket eden ve AEA içinde bulunan bir BCR Üyesinden, Veri İşleyen olarak hareket eden AEA dışındaki başka bir BCR Üyesine yapılan Kişisel Veri Aktarımları.

Aksi takdirde Kişisel Veriler aktarıldığında Concentrix, aktarılan Kişisel Verilerin aşağıda daha ayrıntılı olarak açıklandığı gibi yeterli bir koruma seviyesinden yararlanmasını sağlamak için belirli garantiler uygulayacaktır:

* Veri Sorumlusunun Concentrix’in kendi adına ileriye dönük herhangi bir aktarım dahil bu Aktarımı gerçekleştirmesine izin vermiş olması koşuluyla, Veri İşleyen olarak hareket eden bir BCR Üyesinden Veri İşleyen olarak hareket eden (BCR-P’ye tabi olmayan) bir Concentrix İştirakine veya AEA dışındaki üçüncü taraflara (daha spesifik olarak AB Komisyonu tarafından yeterlilik kararı verilmiş bir AEA dışı ülkeye) yapılan Kişisel Veri Aktarımları, yetkili AEA Denetim Kurumu ve/veya AB Komisyonu (AB Komisyonu Aktarımlar Hakkındaki SCC’ler (914/2021), Modül 3 Veri İşleyenden Veri İşleyene) tarafından kabul edilen geçerli standart sözleşme maddelerini içeren yazılı bir anlaşma ile desteklenecektir.
* Veri Sorumlusunun Concentrix’in kendi adına ileriye dönük herhangi bir aktarım dahil bu Aktarımı gerçekleştirmesine izin vermiş olması koşuluyla, Veri İşleyen olarak hareket eden bir BCR Üyesinden Veri Sorumlusu olarak hareket eden (BCR-P’ye tabi olmayan) bir Concentrix İştirakine veya AEA dışında bulunan üçüncü taraflara (daha spesifik olarak AB Komisyonu tarafından yeterlilik kararı verilmiş bir AEA dışı ülkeye) yapılan Kişisel Veri Aktarımları, yetkili AEA Denetim Kurumu ve/veya AB Komisyonu (AB Komisyonu Aktarımlar Hakkındaki SCC’ler (914/2021), Modül 4 Veri İşleyenden Veri Sorumlusuna) tarafından kabul edilen geçerli standart sözleşme maddelerini içeren yazılı bir anlaşma ile desteklenecektir.
* Yukarıda açıklandığı gibi bir yeterlilik kararı veya uygun güvenlik önlemlerinin bulunmaması durumunda, GDPR Madde 49 uyarınca bir istisna geçerliyse ve ilgili durumlar ara sıra olacak ve tekrarlamayacak şekilde Veri Aktarımları istisnai olarak gerçekleşebilir.

Her halükarda Veri İşleyen olarak hareket eden BCR Üyeleri, öncelikle GDRP ile güvence altına alınan İlgili Kişilerin koruma düzeyinin zayıflatılmamasını sağlamak için aktarılan Kişisel Verilere GDRP ile sağlanan korumayla uyumlu yeterli bir koruma düzeyinin sağlanacağından emin olmadan Kişisel Verileri Concentrix Grubunun bir parçası olmayan üçüncü taraflara Aktarmamayı taahhüt eder.

Anlaşılabilirlik adına, bir BCR Üyesinin Veri İşleyen olarak hareket ettiği durumlarda, BCR Üyesinin tabi olduğu Birlik veya Üye Devlet yasaları tarafından zorunlu tutulmadığı sürece, yalnızca Veri Sorumlusundan alınan belgelenmiş talimatlar uyarınca Veri Aktarımına devam edecektir. Böyle bir durumda, söz konusu yasa Veri Sorumlusunun tabi olduğu Birlik yasasında veya Üye Devlet yasasında tanınan kamu yararı açısından önemli gerekçelerle bu tür bilgileri yasaklamadığı sürece BCR Üyesi, Kişisel Verileri İşlemeden önce Veri Sorumlusunu bu yasal gereklilik hakkında bilgilendirecektir.

* 1. Devletin erişim talebi durumunda Veri Alıcısının yükümlülüğü

Veri Alıcısı olarak hareket eden BCR Üyesinin, Veri Sağlayıcısına BCR-P (aşağıda Madde 13.3) kapsamındaki taahhütlere uyma konusundaki yetersizliğini bildirme yükümlülüğü saklı kalmak üzere Veri Alıcısı olarak hareket eden BCR Üyesi, aşağıdaki durumlarda Veri Sağlayıcısını ve mümkünse İlgili Kişiyi (gerekirse Veri Sağlayıcısının yardımıyla) derhal bilgilendirecektir:

* Hedef ülkenin veya diğer bir üçüncü ülkenin yasaları uyarınca bir resmi kurumdan BCR-P uyarınca aktarılan Kişisel Verilerin ifşası için yasal olarak bağlayıcı bir talep alırsa. Söz konusu bildirim; talep edilen Kişisel Veriler, talep eden kurum, talebin yasal dayanağı ve verilen yanıt hakkında bilgiler içerecektir.
* Hedef ülkenin yasalarına göre BCR-P uyarınca aktarılan Kişisel Verilere resmi kurumların doğrudan erişiminden haberdar olursa. Söz konusu bildirim Veri Alıcısının erişebildiği tüm bilgileri içerecektir.

Veri Sağlayıcısına ve/veya İlgili Kişiye bildirimde bulunması yasaklanırsa Veri Alıcısı, mümkün olduğunca fazla bilgiyi en kısa zamanda iletmek üzere bu yasaktan feragat etmek için en iyi çabayı gösterecek ve Veri Sağlayıcısının talebi üzerine gösterebilmek için çabalarını belgeleyecektir.

Veri Alıcısı, Veri Sağlayıcısı olarak hareket eden BCR Üyesine düzenli aralıklarla alınan talepler konusunda mümkün olduğunca fazla bilgi sağlayacaktır (özellikle talep sayısı, talep edilen veri türü, talep eden kurum(lar) taleplere itiraz edilip edilmediği ve bu itirazların sonucu, vs.). Veri Alıcısının Veri Sağlayıcısına yukarıda belirtilen bilgileri kısmen veya tamamen sağlaması yasaklanırsa Veri Alıcısı, Veri Sağlayıcısını uygun şekilde gecikmeden bilgilendirecektir.

Veri Alıcısı yukarıda belirtilen bilgileri, Kişisel Veriler BCR-P ile sağlanan güvencelere tabi olduğu sürece saklayacak ve talep üzerine Yetkili Denetim Kurumuna sunacaktır.

Veri Alıcısı, ifşa talebinin yasallığını, özellikle de talep eden resmi kuruma verilen yetkiler dahilinde kalıp kalmadığını inceleyecek ve dikkatli bir değerlendirmenin ardından talebin hedef ülkenin yasaları, uluslararası hukuk kapsamındaki geçerli yükümlülükler ve uluslararası nezaket ilkeleri uyarınca hukuka aykırı olduğunu düşünmek için makul gerekçeler olduğuna karar verirse bu talebe itiraz edecektir.

Veri Alıcısı, aynı koşullar altında itiraz olanaklarını gözetecektir.

Bir talebe itiraz ederken Veri Alıcısı, yetkili adli kurum talebin esasına karar verene kadar talebin etkilerini askıya almak amacıyla geçici tedbirler arayacaktır. Veri Alıcısı, geçerli usul kuralları uyarınca bunu yapması gerekene kadar talep edilen Kişisel Verileri ifşa etmeyecektir.

Veri Alıcısı, yasal değerlendirmesini ve ifşa talebine yönelik itirazı belgelendirecek ve hedef ülkenin yasaları uyarınca izin verilen ölçüde belgeleri Veri Sağlayıcısına sunacaktır. Veri Alıcısı, talep edilmesi halinde belgeleri Yetkili Denetim Kurumuna da sunacaktır.

Veri Alıcısı, söz konusu talebin makul yorumuna dayanarak ifşa talebine yanıt verirken izin verilen asgari miktarda bilgiyi sağlayacaktır.

Her halükarda bir BCR Üyesi tarafından herhangi bir resmi kuruma yapılan Kişisel Veri Aktarımları demokratik bir toplumda gerekli olanın ötesine geçecek şekilde büyük çapta, orantısız ve gelişigüzel olamaz (bu konu için bkz. BCR-P Madde 12.3).

1. İlgili Kişinin Hakları
   1. Üçüncü Taraf Lehtar Hakları

Bir BCR Üyesinin Müşterileri adına Veri İşleyen olarak hareket ettiği durumlarda İlgili Kişiler, Kişisel Verilerinin İşlenmesine ilişkin haklarını BCR Üyesinin Müşterilerine karşı kullanabilirler.

Ancak İlgili Kişilerin talebi, Veri İşleyenlere yüklenen gerekliliklerle ilgiliyse İlgili Kişiler en azından aşağıdaki hakları doğrudan BCR Üyelerine karşı uygulayabilmelidir:

* Kişisel Verilerin üçüncü ülkelere aktarılması da dahil olmak üzere Kişisel Verilerin İşlenmesiyle ilgili Veri Sorumlusunun talimatlarına saygı gösterme sorumluluğu (Madde 4.2 ve 6 ),
* Uygun teknik ve organizasyonel güvenlik önlemlerini uygulama yükümlülüğü ve herhangi bir Kişisel Veri İhlalini Veri Sorumlusuna bildirme görevi (Madde 4.5, 4.7 ve 3),
* Bir Alt Veri İşleyen çalıştırırken koşullara uyma görevi (Madde 4.7),
* Veri Sorumlusu ile iş birliği yapma ve İlgili Kişilerin haklarıyla ilgili taleplerine yanıt verme gibi yasalara uyma ve uyumu gösterme konusunda yardımcı olma görevi (Madde 4.6 ve 4.7),
* Concentrix web sitesindeki BCR-P’ye kolay erişim (şu anda www.concentrix.com),
* Dahili şikayet mekanizmaları aracılığıyla şikayette bulunma hakkı (Madde 8),
* AEA Denetim Kurumu ile iş birliği yapma görevi (madde 13.4),
* Sorumluluk, tazminat ve yargı yetkisi hükümleri (Madde 9),
* BCR-P’ye saygı gösterilmesini engelleyen ulusal mevzuat (Madde 4.1, 6.2 ve 13.3),
* Üçüncü taraf lehtar haklarının uygulanabilirliğini sağlama görevi (Madde 7).

Her halükarda İlgili Kişiler:

* İşbu BCR-P ve/veya Geçerli Veri Koruma Mevzuatı kapsamında garanti altına alınan hakların ihlali için yargısal çözümler arama hakkına sahiptir (Madde 9).
* BCR-P’nin herhangi bir BCR Üyesi tarafından ihlalinden kaynaklı zarar (maddi zarar ve sıkıntı dahil) için telafi ve uygun olduğu hallerde tazminat alma hakkına sahiptir (Madde 9).
* AEA Denetim Kurumuna veya AEA’da bulunan Müşteri için yetkili mahkemelere şikayette bulunma hakkına sahiptir (Madde 7.1. ve 7.2).

Concentrix’in diğer müracaatlarına halel getirmeksizin, aynı Veri İşleme sürecine dahil olan Veri İşleyen ve Veri Sorumlusunun bu Veri İşlemeden kaynaklanan bir zarardan sorumlu bulunması halinde İlgili Kişi, doğrudan Veri İşleyen olarak hareket eden BCR Üyesinden tüm zararın tazminini alma hakkına sahiptir.

Müşterinin fiilen ortadan kaybolduğu veya hukuken artık var olmadığı veya iflas ettiği ve başka hiçbir kuruluşun Müşterinin yükümlülüklerini tahsil etmek için yasal yükümlülük üstlenmediği kanıtlanabildiği takdirde İlgili Kişiler, aşağıdaki hakları kullanma ve Veri İşleyen olarak hareket eden ve Müşteri ile bir Hizmet Sözleşmesi ile bağlı olan BCR Üyesine karşı doğrudan dava açma hakkına sahiptir:

* BCR-P’nin uygulanabilir unsurlarına uyma görevi (Madde 3.1 ve 3.2),
* Üçüncü taraf lehtar haklarının uygulanabilirliğini sağlama görevi (Madde 7),
* Webhelp SAS tarafından i) tazminat ödeme ve AEA dışındaki bir BCR Üyesi tarafından tazmin edilebilir bir zararla sonuçlanan şekilde BCR-P’ye uyulmaması durumunda çare sunma yükümlülüğünün ii) ilgili BCR Üyesinin İlgili Kişi tarafından talep edilen zararlarla sonuçlanan BCR-P’nin ihlali iddiasından sorumlu olmadığını gösterme yükümlülüğünün onaylanması (Madde 7.2),
* Concentrix web sitesindeki BCR-P’ye kolay erişim (şu anda www.concentrix.com),
* Şirketlerin dahili şikayet mekanizması aracılığıyla şikayette bulunma hakkı (Ek 5 – Madde 3.1),
* AEA Denetim Kurumu ile iş birliği görevleri (Madde 13.4),
* Veri Sorumlusu ile iş birliği yapma görevi (Madde 4.1),
* Madde 4’te listelenen Kişisel Verilerin İşlenmesine ilişkin ilkelere uyma görevi,
* BCR’ye tabi kuruluşların listesini kullanıma sunmak ve güncellemek (Ek 1) ve
* BCR-P’ye saygı gösterilmesini engelleyen ulusal mevzuat (Madde 13.3).

Bir BCR Üyesi, İlgili Kişilerin adına şikayette bulunmak, yukarıda bahsedilen hakları kullanmak için kar amacı gütmeyen bir kuruluş, organizasyon veya dernek tarafından temsil edilebileceğini kabul eder. Söz konusu kuruluş, organizasyon veya dernek, bir Üye Devletin yasalarına uygun şekilde kurulmuş olmalı, kamu yararına yasal amaçlara sahip olmalı ve İlgili Kişilerin Kişisel Verilerinin korunmasına ilişkin hak ve özgürlüklerinin korunması alanında faaliyet göstermelidir.

Anlaşılabilirlik adına, yukarıda açıklanan üçüncü taraf lehtar haklarının eğitim, denetim programı, uyumluluk ağı ve BCR-P güncelleme mekanizması gibi kuruluşlar içinde uygulanan iç mekanizmalara ilişkin BCR-P’nin bu unsurlarına uzanmadığı belirtilmiştir.

**İşbu Madde 7 hükümlerine halel gelmeksizin, Concentrix’in İlgili Kişileri aşağıda BCR Madde 8’de açıklanan dahili şikayet mekanizmasını kullanmaya teşvik ettiğini unutmayın.**

* 1. AEA dışındaki bir BCR Üyesinin BCR-P’ye uymaması durumunda şikayette bulunma ve yargısal çözüm, düzeltme ve tazminat alma hakkı

AEA dışındaki bir BCR Üyesinin BCR-P’ye uymaması durumunda Webhelp SAS (1) yetkili mahkeme tarafından verildiğinde tazminat ödemesi de dahil olmak üzere BCR-P’ye uyulmamasından kaynaklı zararlardan sorumlu olduğunu onaylar ve (2) söz konusu diğer BCR Üyesinin eylemlerini düzeltmek için gerekli aksiyonları almayı kabul eder.

Bu tür durumlarda Webhelp SAS, İlgili Kişinin aşağıdaki hususlarda hak sahibi olduğunu da kabul eder:

* İkametgahı ve iş yerinin bulunduğu veya devredilmiş sorumluluğa sahip BCR Üyesinin kurulduğu yerde bir Denetim Kurumuna şikayette bulunmak ve/veya
* İlgili Kişinin Veri İşleyen olarak hareket eden herhangi bir BR Üyesi tarafından kendisiyle ilgili Kişisel Verilerin İşlenmesinin işbu BCR-P’yi ihlal ettiğini düşünmesi halinde etkili bir yargısal çözüm. BCR Üyeleri, bu talebin BCR-P’ye uyulmamasından sorumlu olan BCR Üyesinin kurulduğu Üye Devlette veya İlgili Kişinin daimi ikametgahının bulunduğu mahkemede ileri sürülebileceğini kabul eder.

Webhelp SAS, AEA dışındaki BCR Üyesinin işbu BCR-P kapsamında belirtilen kuralların ihlal edilmesinden sorumlu olmadığını ve bu durumun İlgili Kişinin tazminat talebine yol açtığını göstermekten sorumlu olacaktır. Webhelp SAS, AEA dışında bulunan diğer BCR Üyesinin bu fiilden sorumlu olmadığını gösterebilirse kendisini her türlü sorumluluktan kurtarabilir.

Veri Sorumlusu zarar gördüğünü gösterebilir ve bu zararın AEA dışındaki bir BCR Üyesinin işbu BCR-P’yi ihlali nedeniyle meydana gelmiş olma ihtimalinin yüksek olduğunu kanıtlarsa Webhelp SAS, AEA dışındaki BCR üyesinin veya AEA dışındaki harici Alt Veri İşleyenin söz konusu zararlara yol açan BCR-P ihlalinden sorumlu olmadığını veya böyle bir ihlalin gerçekleşmediğini göstermekten sorumlu olacaktır.

* 1. İlgili Kişilerin Hakları

İlgili Kişiler aşağıdaki haklardan yararlanma hakkına sahiptir:

* Kendisiyle ilgili ve bir BCR Üyesi tarafından İşlenen Kişisel Verilere erişim,
* Kendisiyle ilgili yanlış veya eksik Kişisel Veriler ile Veri İşleme amacının artık yasal veya uygun olmadığı Kişisel Verilerin düzeltilmesi veya silinmesi talebi,
* Kendisiyle ilgili Kişisel Veri İşlemenin sınırlandırılmasını talep etme,
* Söz konusu İşlemenin Veri Sorumlusunun gözettiği meşru menfaat amaçları için gerekli olması durumunda, Veri Sorumlusu olarak hareket eden Müşterinin gözettiği menfaatler İlgili Kişilerin menfaat hak ve özgürlüklerini geçersiz kılmadığı sürece kendi kişisel durumuyla ilgili gerekçelerle dilediği zaman profilleme dahil meşru menfaat amaçları için Kişisel Verilerinin bir BCR Üyesi tarafından İşlenmesine itiraz etme,
* Söz konusu İşlemenin Veri Sorumlusu veya bir üçüncü tarafın gözettiği meşru menfaat amaçları için gerekli olması durumunda, profilleme dahil pazarlama amaçları için Kişisel Verilerinin bir BCR Üyesi tarafından İşlenmesine itiraz etme,
* Kişisel Verilerini yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilen bir biçimde ve İşleme otomatik yollarla gerçekleştirildiğinde birlikte işlem görebilir şekilde alma.

Bir BCR Üyesi, Veri İşleyen olarak hareket ederken İlgili Kişilerden haklarını kullanmak üzere bir talep alırsa Müşterisini bu konuda bilgilendirecek ve Müşteri ise talebe yanıt verecektir. BCR Üyesi yalnızca Müşterisinin bu tür taleplerin nasıl ele alınacağına ilişkin diğer talimatlarına uymaktan sorumludur. BCR Üyeleri, kimlik tespit formunun artık gerekli olmadığı andan itibaren Kişisel Verilerin güncellenmesi, düzeltilmesi, silinmesi veya anonimleştirilmesi için Müşteri tarafından istenen tüm gerekli önlemleri uygulayacaktır. BCR Üyeleri, bu talimatları Kişisel Verilerin açıklandığı ilgili tüm BCR Üyelerine iletecektir. BCR Üyeleri ayrıca mümkün olduğu ölçüde yararlı bilgileri iletmek de dahil olmak üzere taleplere yanıt verme yükümlülüğünü yerine getirmek için Müşterilerin talimatlarını izleyerek uygun teknik ve organizasyonel önlemleri uygulayacaktır. Müşteri ortadan kaybolduğunda ya da varlığını yitirdiğinde veya iflas ettiğinde, ilgili BCR Üyesi söz konusu talebi mümkün olduğunca ve benimsediği prosedüre uygun olarak doğrudan ele alacaktır.

* 1. İlgili Kişilerin Haklarının Kullanılması

İlgili Kişiler, işbu BCR-P’yi üçüncü taraf lehtar olarak uygulama ve Kişisel Verilerinin Veri İşleyen olarak hareket eden herhangi bir BCR Üyesi tarafından İşlenmesiyle ilgili haklarını kullanma hakkına sahiptir. BCR Üyesi, İlgili Kişinin haklarının kullanımına ilişkin herhangi bir talebinin veya şikayetinin (“**Talepler**”) zamanında ele alınmasını sağlayacaktır.

İlgili Kişiler sözlü veya yazılı olarak talepte bulunabilir. BCR Üyeleri, İlgili Kişilere haklarını kullanabilecekleri erişilebilir araçlar ve özellikle:

1 - İlgili Kişinin bulunduğu ülkeden bağımsız olarak kullanabileceği tek bir özel iletişim e-postası sağlayacaktır:

[dpo@concentrix.com](mailto:dpo@concentrix.com)

Kullanılan dil gibi yerel özellikleri dikkate almak için yerel e-postalar kullanılabilir.

Yerel gizlilik irtibat kişinize ulaşmak için lütfen Ek 01 - BCR-P’ye tabi Concentrix kuruluşları ve yerel Gizlilik e-posta iletişim listesi dokümanına bakınız.

2 - www.concentrix.com adresindeki bir köprü metni aracılığıyla erişilebilen Concentrix DPO e-posta adresinin bulunduğu tek bir portal

3 - İlgili Kişinin bulunduğu ülkeden bağımsız olarak kullanabileceği tek özel posta adresi:

Group Data Privacy Officer (Grup Veri Koruma Görevlisi)

Legal and Compliance Department (Hukuk ve Mevzuat Uyum Departmanı)

3 rue d’Heliopolis

75017 – PARİS

FRANSA

DPO veya DPO’nun Talepleri yönetmek üzere atadığı, kurum içi veya dışı, herhangi bir diğer kişi veya kuruluş, (i) söz konusu İlgili Kişiden Talebini ele almak için gerekli asgari bilgilerin alınmasını sağlayacak ve (ii) gerekli görüldüğü takdirde, Talebin usulüne uygun şekilde ele alınmasını sağlamak için mümkün olduğunca fazla bilgi edinecektir.

Talepte bulunan kişinin kimliği konusunda şüphe varsa özellikle uzaktan iletişim araçları kullanıldığında, bir BCR Üyesinin İlgili Kişiler hakkında daha fazla bilgi istemesi gerekebilir. Toplanan bilgiler (i) talepte bulunan kişinin kim olduğunu doğrulamak için gerekli olan bilgilerle sınırlı olacak ve (ii) bir BCR Üyesi veya Müşterileri tarafından sağlanan ürün veya hizmetler kullanıcının gerçek kimliği altında teslim edilmediğinde toplanmayacaktır. Orantılılık her zaman Veri Sorumlusu tarafından değerlendirilecektir.

Her durumda, Talebin alınmasından itibaren en geç 1 ay içinde İlgili Kişiye yanıt verilmelidir. Taleplerin karmaşıklığı ve sayısı dikkate alındığında, bu bir aylık süre en fazla iki ay daha uzatılabilir; bu durumda şikayetçi buna göre bilgilendirilmelidir (Ek 6’da ayrıntılı olarak açıklandığı üzere).

İlgili Kişi, BCR Üyesi tarafından sağlanan ilk yanıttan memnun kalmazsa her halükarda Talebinin yeniden incelenmesini derhal talep etme hakkına sahip olacaktır. İlgili Kişi, BCR Üyesine daha önce sağlanan çözümün yeterli olmayan hükümlerine dair ayrıntılı bir açıklama sunacaktır. BCR Üyesi, Talebin alınmasından itibaren en geç 2 ay içinde talebin nasıl ele alınacağını belirlemek için yeniden incelemeyi dikkate alacak ve İlgili Kişiyi bu konuda yazılı olarak bilgilendirecektir.

İlgili Kişinin Talebi veya şikayeti, BCR Üyesi tarafından reddedilir veya verilen yanıt İlgili Kişinin talebini karşılamazsa İlgili Kişi, DPO ile iletişime geçebilir ve/veya doğrudan yetkili bir AEA Denetim Kurumuna şikayette bulunabilir ve/veya yargı yoluna başvurabilir.

İşbu Madde ile ilgili daha fazla ayrıntı aşağıdaki ekte mevcuttur:

* **Ek 6 - Concentrix’in Veri İşleyen olarak hareket ettiği durumlarda İlgili Kişilerin taleplerine ilişkin prosedür**

1. İlgili Kişilerin şikayet yönetimi prosedürü

İlgili Kişi bir şikayeti doğrudan BCR Üyesine ilettiğinde ancak BCR Üyesi bu talebi aldığında Müşteri varlığını yitirmemiş, ortadan kaybolmamış veya iflas etmemişse BCR Üyesi, Müşteriyi bu talep hakkında gecikmeden ve **Ek 6 -** **Concentrix’in Veri İşleyen olarak hareket ettiği durumlarda İlgili Kişilerin taleplerine ilişkin prosedür** kapsamında tanımlanan prosedüre uygun olarak bilgilendirmeyi taahhüt eder.

Böyle bir durumda BCR Üyesi, İlgili Kişiden aldığı bilgileri Müşteriye iletmeyi taahhüt eder ve Müşteriye söz konusu şikayeti ele almanın Müşterinin sorumluluğunda olduğunu açıkça belirtmeyi kabul eder.

Concentrix, Veri İşleyen olarak hareket ederken İlgili Kişilerin şikayetlerini ele almaktan sorumlu değildir. Bununla birlikte Müşteri fiilen ortadan kaybolmuşsa, hukuken varlığını yitirmişse veya iflas etmişse BCR Üyeleri, İlgili Kişilerden gelen şikayetleri BCR-P Madde 8 kapsamında belirtilen aynı prosedüre uygun olarak ele almayı taahhüt eder. Bu durumda BCR Üyeleri, İlgili Kişilerin bir AEA Denetim Kurumu nezdinde dava açma ve/veya yargısal çözüm arama hakkına sahip olmaya devam ettiğini kabul eder. BCR Üyeleri ayrıca bu hakların İlgili Kişilerin şikayet yönetimi sürecini daha önce kullanmış olmalarına bağlı olmadığını kabul eder ancak İlgili Kişiler bunu yapmaya yeniden teşvik edilir.

1. Harici Müşterilerin Şikayetleri

Veri İşleyen olarak hareket eden bir BCR Üyesi işbu BCR-P’ye uymuyorsa Concentrix, Müşterinin işbu BCR-P’yi aykırı hareket eden BCR Üyesine karşı uygulama hakkına sahip olduğunu kabul eder.

Hizmet Sözleşmesi ve/veya Veri İşleme Sözleşmesi hükümlerine tabi olarak, Müşteri yargısal çözümlere hak kazanır ve ihlalin başlangıç noktasında BCR Üyesinden tazminat alma hakkına sahiptir.

1. Veri koruma yönetimi

Concentrix, Ek 3’te daha ayrıntılı olarak tanımlanan bir Veri koruma organizasyonu ve yönetimi tanımlamıştır.

BCR Üyeleri, gerektiğinde ve GDPR Madde 37 uyarınca bir Veri Koruma Görevlisi veya BCR-P’ye uyumu izlemekten sorumlu olan ve bu görevin yerine getirilmesinde en yüksek yönetim desteğini alan (Grup baş gizlilik sorumlusu gibi) başka bir kişi veya kuruluş atamayı taahhüt eder. Bu organizasyon, gizlilik iletişim noktalarından (yani Bölgesel Gizlilik Liderleri, Yerel Gizlilik Liderleri ve İş Gizlilik Uzmanları) oluşan bir ağa dayanan ve ilgili BCR Üyesi tarafından DPO olarak atanabilecek olan Grup Veri Koruma Görevlisi tarafından yönetilir.

Bir Denetim Kurumu tarafından resmi olarak atanan DPO, doğrudan en üst yönetim seviyesine rapor verecektir. Ayrıca DPO, görevlerini yerine getirirken herhangi bir soru veya sorun ortaya çıkarsa en üst yönetim seviyesini bilgilendirebilir.

DPO’nun çıkar çatışmasına yol açabilecek hiçbir görevi olmamalıdır. DPO ne veri koruma etki değerlendirmelerini yürütmekten ne de söz konusu durumlar bir çıkar çatışmasına yol açabilecekse BCR denetimlerini yürütmekten sorumlu olmalıdır. Bununla birlikte DPO, BCR Üyelerine yardımcı olmakta çok önemli ve yararlı bir rol oynayabilir ve bu tür görevler için DPO tavsiyesi alınmalıdır.

Mevcut ağın görev ve sorumlulukları ile çalışma yönetimi, **Ek 3 - Veri Koruma organizasyonu ve yönetimi** kapsamında daha ayrıntılı olarak tanımlanmıştır.

Ayrıca DPO, görevlerini yerine getirirken herhangi bir soru veya sorun ortaya çıkarsa en üst yönetim seviyesini bilgilendirebilir.

DPO’ya ve Bölgesel ve/veya Yerel Gizlilik Liderlerine, BCR-C Madde 7.4’te açıklanan iletişim bilgilerinden ve BCR Ek 01’de verilen yerel gizlilik irtibat kişilerinden ulaşılabilir.

1. Eğitim ve farkındalık

Kişisel Verilerin Korunması yalnızca gizlilik yasalarına uyum meselesi değil, aynı zamanda Concentrix temel değerlerinin somutlaşmış halidir. Bu bağlamda tüm çalışanları, stajyerleri ve çalışma performansındaki davranışları BCR Üyelerinin doğrudan kontrolü altında olan diğer kişileri operasyonları kapsamında İşlenen Kişisel Verilerin korunmasından sorumlu tutmak için Grup içinde bir gizlilik kültürü oluşturulması esastır.

Bu nedenle işbu BCR-P tüm kuruluş içinde uygun şekilde uygulanacaktır. Bu amaçla BCR Üyeleri; tüm Concentrix çalışanlarının, stajyerlerinin ve çalışma performansındaki davranışları BCR Üyelerinin doğrudan kontrolü altında olan diğer kişilerin işbu BCR-P’de belirtilen yükümlülük, ilke ve prosedürler hakkında gerçekten bilgi sahibi olmasını sağlamayı amaçlayan bir gizlilik eğitim programı benimsemiştir. Temel GDPR ilke ve yükümlülüklerine ek olarak, eğitim ve farkındalık programı diğerlerinin yanı sıra kamu kurumları tarafından kişisel verilere erişim taleplerinin yönetilmesine yönelik prosedürleri kapsayacaktır.

Bu eğitim; (i) Kişisel Verilere kalıcı veya düzenli erişimi olan kişilere, (ii) Kişisel Verilerin toplanmasında yer alan kişilere ve/veya (iii) Kişisel Verileri işlemek için kullanılan araçların geliştirilmesinde yer alan kişilere yöneliktir.

Eğitim materyali güncel olacak ve BCR-P’nin en son versiyonunu yansıttığından emin olmak için en azından yılda bir kez veya geçerli Veri Koruma Mevzuatında önemli değişiklikler olduğunda düzenli olarak gözden geçirilecektir.

Eğitim programının amacı şunları sağlamak olacaktır:

* Kişisel Verilerin İşlenmesinde geçerli ilkeler hakkında temel düzeyde bilgi ve mevcut prosedürler ve bunların uygulanması hakkında iyi bir anlayış,
* Kuruluş bünyesindeki farklı fonksiyonlara uyarlanmış özel eğitim.

Bu bağlamda BCR Üyelerinin BCR-P kapsamında başka bir BCR Üyesine, BCR-P’ye etkin bir şekilde tabi olmadıkça ve çalışanlarına etkili bir şekilde BCR-P hakkında uygun bir eğitim sağlamadıkça hiçbir veri aktarımı yapılamayacağını kabul ettikleri hatırlatılır.

BCR Üyeleri tüm Concentrix çalışanları, stajyerleri ve çalışma performansındaki davranışları BCR Üyelerinin doğrudan kontrolü altında olan diğer kişilerin işe ilk girdiklerinde bu eğitimi ve ardından da her yıl tazeleme eğitimi almasını sağlamayı taahhüt eder.

Bu Madde ile ilgili daha fazla ayrıntı aşağıdaki ekte verilmiştir:

* **Ek 04 – Gizlilik farkındalığı ve eğitim programı**

1. Kasten gizlilik/varsayılan gizlilik

BCR Üyeleri, Veri İşleyen olarak hareket ettiklerinde Müşterinin kasten Gizlilik ve varsayılan Gizlilik ile ilgili yükümlülüklerine uymasını sağlamak için Müşteriden gelen makul talimatları takip edecektir.

1. Şeffaflık ve iş birliği
   1. BCR-P İletişimi

BCR Üyeleri, tüm İlgili Kişilere Kişisel Verilerinin İşlenmesiyle ilgili olarak üçüncü taraf lehtar hakları ve bu hakları kullanma yolları hakkında bilgi sağlanacağını taahhüt eder. Söz konusu bilgiler, BCR-P Madde 7’de açıklanmıştır.

Concentrix, işbu BCR-P’yi İlgili Kişilere açık bir şekilde iletecek ve her bireyin buna kolayca erişebilmesini sağlayacaktır. Bu iletişim, İlgili Kişilerin BCR-P’nin bir kopyasını gecikmeksizin ve açık doküman formatında almasını sağlayacaktır.

Buna ek olarak, işbu BCR-P’nin en son sürümünün kamuya açık bir versiyonu İlgili Kişilere her zaman Concentrix web sitesi [www.concentrix.com](http://www.concentrix.com) adresinden sunulacaktır. İlgili Kişiler ayrıca [dpo@concentrix.com](mailto:dpo@concentrix.com) adresinden DPO ile iletişime geçerek BCR-P’nin bir kopyasını talep edebilirler.

BCR-P’nin kamuya açık versiyonu en azından aşağıdaki bilgileri içerecektir:

* BCR-P kapsamına ilişkin bir açıklama (BCR-P Madde 2),
* Grubun yükümlülüğüne ilişkin madde (BCR-P Madde 7),
* Veri koruma ilkelerine ilişkin maddeler (BCR-P Madde 4 ve 5),
* Güvenlik ve kişisel veri ihlali bildirimleri (BCR-P Madde 4.5),
* Alt Veri İşleyen ve ileriye dönük aktarımlara ilişkin kısıtlamalar (BCR-P Madde 4.7 ve Madde 6) ve
* İlgili kişilerin haklarına ilişkin maddeler (BCR-P Madde 7, 8 ve 13).

Bu bilgiler güncel olmalı ve İlgili Kişilere açık, anlaşılır ve şeffaf bir şekilde sunulmalıdır. Bu bilgiler eksiksiz olarak sağlanmalıdır, bu nedenle özetlenmesi yeterli olmayacaktır.

Kamuya açık versiyon, BCR-P’ye Ek belge olarak eklenen tüm gerekli politika ve prosedürleri de içerecektir ama özellikle BCR-P için:

* Ek 01 - A BCR-P’ye tabi olan BCR Üyeleri ve yerel gizlilik e-posta iletişim listesi
* Ek 02 Bağlayıcı Şirket Kuralları (BCR) ve Prosedür Tanımları
* Appendix 06 Concentrix’in Veri İşleyen olarak hareket ettiği durumlarda İlgili Kişilerin taleplerine ilişkin prosedür
* Appendix 11-B BCR-P maddi kapsamı: Veri İşleme Amaçları ve ilgili Kişisel Veri ve İlgili Kişiler Kategorileri Listesi

Diğer Ekler ya BCR-P için geçerli değildir ya da İlgili Kişilerin haklarını anlamaları ve/veya kullanmaları için ilgili olmayan dahili süreçlerdir.

Yukarıdaki gereklilikler, daha önce listelenen tüm bilgileri içeren BCR-P’nin basitleştirilmiş kamuya açık bir versiyonunun Concentrix web sitesinde (www.concentrix.com) bulunmasının sağlanmasıyla karşılanacaktır.

BCR Üyeleri, Veri İşleyen olarak hareket ederken işbu BCR-P’yi Müşterileriyle paylaşmayı taahhüt eder ve BCR-P’yi açıklamak ve yürürlüğe koymak için Hizmet Sözleşmesine dahil eder. Her halükarda BCR-P Madde 3 ve 4’te belirtildiği üzere BCR Üyeleri, Veri İşleyen olarak hareket ettiklerinde Müşterilerinin Kişisel Verilerinin İşlenmesiyle ilgili olarak BCR-P’ye uymayı taahhüt eder.

* 1. İlgili Kişilere Sağlanan Bilgiler

Veri İşleyen olarak hareket eden BCR Üyeleri, Müşterilerine İlgili Kişilere Geçerli Veri Koruma Mevzuatı uyarınca gerekli olan bilgileri vermelerine imkan tanıyacak olan bilgileri sağlamaktan sorumludur.

Bununla birlikte, BCR Üyeleri Geçerli Veri Koruma Mevzuatı uyarınca gerekli olan zorunlu bilgileri İlgili Kişilere sağlamaktan sorumlu olmayacaktır çünkü bu konuda yalnızca BCR Üyelerinin Müşterileri sorumludur.

* 1. BCR-P’ye uyumu etkileyen yerel mevzuat ve uygulamalarla tutarsızlıklar

BCR Üyeleri, BCR-P’yi yalnızca Veri Alıcısı olarak hareket eden BCR Üyesi tarafından Kişisel Verilerin İşlenmesine uygulanabilir olan Yetersiz üçüncü bir hedef ülkedeki yasa ve uygulamaların, Kişisel Verileri ifşa etme gereklilikleri veya kamu otoriteleri tarafından erişime izin veren önlemler dahil olmak üzere, bu BCR-P kapsamındaki yükümlülüklerini yerine getirmesini engellemediğini değerlendirdikleri durumlarda Veri Aktarımları için bir araç olarak kullanmayı taahhüt ederler.

Söz konusu taahhüt, temel hak ve özgürlüklerin özüne saygı gösteren ve aşağıda listelenen amaçlardan birini korumak için demokratik bir toplumda gerekli ve orantılı olanı aşmayan yasa ve uygulamaların BCR-P ile çelişmediği anlayışına dayanmaktadır:

1. Ulusal güvenlik ve/veya
2. Savunma ve/veya
3. Kamu güvenliği ve/veya
4. Suçların önlenmesi, soruşturulması, tespiti veya kovuşturulması veya kamu güvenliğine yönelik tehditlerin önlenmesi ve bunlara karşı koruma sağlanması da dahil olmak üzere cezai yaptırımların uygulanması ve/veya
5. Birliğin veya bir Üye Devletin genel kamu menfaatinin diğer önemli hedefleri, özellikle Birliğin veya bir Üye Devletin parasal, bütçesel ve vergi konuları, kamu sağlığı ve sosyal güvenlik de dahil olmak üzere önemli bir ekonomik veya mali menfaati ve/veya
6. Yargı bağımsızlığının ve adli muamelelerin korunması ve/veya
7. Düzenlemeye tabi meslekler için etik kural ihlallerinin önlenmesi, soruşturulması, tespiti ve kovuşturulması ve/veya
8. (a) ila (e) ve (g) noktalarında belirtilen durumlarda, ara sıra bile olsa, resmi otoritenin uygulanmasıyla bağlantılı bir izleme, teftiş veya düzenleyici işlev ve/veya
9. İlgili Kişinin veya başkalarının hak ve özgürlüklerinin korunması ve/veya
10. amme hukuku kapsamındaki hak taleplerinin yerine getirilmesi.

BCR-P’de yer alan taahhütlere saygı duyulmasını etkileyebilecek Yetersiz Üçüncü bir Ülkenin yasa ve uygulamalarının değerlendirilmesinde, BCR Üyeleri özellikle aşağıdaki unsurları dikkate alacaktır:

* **Veri Aktarımları veya Aktarım setinin özel koşulları** ve aşağıdakiler dahil olmak üzere aynı üçüncü ülke içinde veya başka bir Yetersiz Üçüncü ülkeye öngörülen ileriye dönük Veri Aktarımlarının özel koşulları:
* Kişisel Verilerin aktarılma ve işlenme amaçları (ör. depolama, BT desteği, Müşteri adına müşteri desteği gibi iş süreci dış kaynak hizmetleri),
* Veri İşleme sürecine dahil olan kuruluş türleri (Veri Alıcısı ve herhangi bir ileriye dönük Aktarımın daha sonraki alıcısı),
* Veri Aktarımı veya Aktarım setinin gerçekleştiği ekonomik sektör,
* Aktarılan Kişisel Verilerin kategorileri ve biçimi,
* Depolama dahil olmak üzere Veri İşlemenin yeri ve
* Kullanılan iletim kanalları.
* **Hedef üçüncü ülkenin yasa ve uygulamaları**; verilerin kamu kurumlarına açıklanmasını veya bu kurumlar tarafından erişime izin verilmesini gerektirenler ve Veri Sağlayıcısı ülke ile Veri Alıcısı ülke arasındaki aktarım sırasında bu Kişisel Verilere erişim sağlayanlar da dahil olmak üzere Aktarımın koşulları ışığında ilgili olan hedef üçüncü ülke yasa ve uygulamaları ile geçerli sınırlamalar ve güvenlik önlemleri.
* **İlgili akdi, teknik veya organizasyonel güvenlik önlemleri**; hem veri aktarımı sırasında uygulanan hem de hedef ülkede Kişisel Verilerin İşlenmesine uygulanan önlemler dahil BCR-P kapsamındaki güvenlik önlemlerini tamamlamak için uygulananlar.

Yukarıdakileri göz önünde bulundurarak, bir BCR Üyesinin yukarıdaki Madde **Erreur ! Source du renvoi introuvable.**’de ayrıntılı olarak açıklanan Veri İşleme ilkelerinden herhangi biri dahil yerel mevzuatının işbu BCR-P kapsamındaki yükümlülüklerini yerine getirmesini engellediğine inanmak için nedenleri varsa ve burada sağlanan garantiler üzerinde önemli bir etkisi varsa söz konusu BCR Üyesi derhal (i) Müşteri(ler)sini, (ii) Webhelp SAS’ı, (iii) devredilmiş veri koruma sorumluluklarına sahip AB BCR Üyesini ve (iv) DPO’yu veya ilgili Yerel Gizlilik Liderini / diğer gizlilik fonksiyonunu bilgilendirmelidir.

Bir BCR Üyesi, Veri İşleyen olarak hareket ettiğinde böyle bir durumda Müşterisi için yetkili veri koruma kurumunu derhal bilgilendirmeyi de taahhüt eder.

İlgili BCR Üyesi iletişim noktası(ları) yukarıda belirtilen bildirim mekanizmasına göre bilgilendirildiğinde, Webhelp SAS yetkili AEA Denetim Kurumunu bilgilendirecektir. Böyle bir durumda, Webhelp SAS ilgili yetkili AEA Denetim Kurumunu bu yasal gereklilik hakkında fazla gecikmeden bilgilendirmeyi ve söz konusu yasal gereklilikler ilgili BCR Üyesi tarafından Kişisel Verilerin ifşa edilmesini zorunlu kıldığında, yalnızca ilgili yerel mevzuata uygun olarak gerekli Kişisel Verileri ifşa etmeyi taahhüt eder. BCR Üyeleri, bu yasal gereklilik veya ifşanın hangi İlgili Kişileri ilgilendirebileceğini, hangi kurumun bu açıklamayı talep ettiğini ve hangi yasal temele dayandığını belirtecektir. Her durumda BCR Üyeleri, Kişisel Verileri kamu kurumlarına büyük çapta, gelişigüzel ve orantısız bir şekilde aktarmamayı taahhüt eder.

Bir BCR Üyesinin böyle bir bildirimi yapması yasal olarak yasaklanmışsa, geçerli yerel mevzuata uygun olarak bu yasaktan feragat etmek için elinden gelen çabayı göstermelidir. Webhelp SAS ve bu BCR Üyesi, Müşteriyi ve ilgili AEA Denetim Kurumlarını bilgilendirebilmek amacıyla bu yasağı aşmak için azami çabayı gösterecektir. BCR Üyeleri, yasaktan feragat etmek üzere azami çabayı göstermek için bu amaçla alınan aksiyonu belgeleyecek ve ilgili AEA Denetim Kurumuna sunacaktır. Bu yasağı aşmanın mümkün olmadığı durumlarda Webhelp SAS, ilgili kurumlara Kişisel Verilerin açıklanma sayıları hakkında yıllık genel bilgiler sağlamalıdır (ör. bilgi ifşası için yapılan başvuru sayısı, talep edilen veri türü, mümkünse talep eden, vs.).

Bunun yanı sıra bir BCR Üyesi, işbu BCR-P kapsamında bir BCR Üyesi tarafından gerçekleştirilen Veri İşleme üzerinde etkisi olabilecek bazı gereklilikler veya usuller ekleyen AB Üye Devletleri ulusal mevzuatına tabi olduğunda, bu BCR Üyesi derhal Webhelp SAS’ı bilgilendirecek ve bu ulusal mevzuat kapsamında geçerli olan tamamlayıcı gereklilikleri belgelendirecektir. Bu ulusal mevzuat Kişisel Veriler için daha yüksek düzeyde koruma getirdiğinde bu ulusal mevzuat, BCR-P’ye göre öncelikli olacaktır.

AEA dışında bulunan bir BCR Üyesinin yukarıda belirtilen değerlendirmeye uygun olmayan yasalara veya uygulamalara tabi olduğuna inanmak için nedenleri varsa, derhal Müşteriye veya söz konusu Müşteri adına Veri İşleyen olarak hareket eden ve bu bildirimi Müşteriye iletecek olan AB BCR Üyesine bildirimde bulunmalıdır. Bildirimin ardından Müşteri ve/veya Veri İşleyen olarak hareket eden AB BCR Üyesi, durumu ele almak için benimsenmesi gereken uygun önlemleri (ör. güvenliği ve gizliliği sağlamak için teknik veya organizasyonel önlemler) derhal belirlemelidir. Söz konusu Veri Aktarımı için uygun bir güvenlik önlemi sağlanamazsa Aktarım askıya alınacaktır. Bu durumda Müşteri ve/veya AB BCR Üyesi, işbu BCR-P kapsamındaki kişisel verilerin işlenmesiyle ilgili olduğu ölçüde sözleşmeyi feshetme hakkına sahip olacaktır. Sözleşme ikiden fazla tarafı içeriyorsa Müşteri ve/veya AB BCR Üyesi, taraflar aksi şekilde anlaşmadığı sürece, yalnızca ilgili BCR Üyesinin Kişisel Verilere yeterli düzeyde koruma sağlayamaması durumunda bu fesih hakkını kullanabilir.

* 1. İş birliği yapma görevi

Her durumda BCR Üyeleri, Denetim Kurumları tarafından denetlenmeyi veya (yerinde veya uzaktan) teftiş edilmeyi kabul etmek suretiyle dahil olmak üzere AEA Denetim Kurumlarıyla iş birliği yapmayı, tavsiyeleri dikkate almayı ve işbu BCR-P ile ilgili olarak sağlanabilecek yetkili EEA Denetim Kurumunun kararına tabi olmayı kabul eder. BCR Üyeleri, yetkili Denetim Kurumunun yetkileri ve denetim haklarının, özellikle söz konusu Denetim Kurumu tarafından yürütülen pratik denetimle ilgili olarak sınırlandırılamayacağını kabul eder ve onaylar.

BCR Üyeleri, Alt Veri İşleyen olarak hareket ettiklerinde makul bir süre içinde ve mümkün olduğu ölçüde Müşterileriyle iş birliği yapmayı ve Müşterilerinin Geçerli Veri Koruma Mevzuatına uymalarına yardımcı olmayı taahhüt eder. BCR Üyeleri ayrıca Kişisel Verileri İşlemek için kullandığı herhangi bir Alt Veri İşleyenin, BCR Üyelerine ve gerektiğinde Veri Sorumlusuna iş birliği yapma ve yardımcı olma konusunda aynı görevi yerine getirmekle yükümlü olduğundan emin olacaktır.

BCR Üyeleri ve uygun olduğunda ilgili temsilcileri, talep edilmesi halinde BCR-P kapsamındaki veri işleme faaliyetlerine ilişkin kayıtlar gibi bilgileri AEA Denetim Kurumuna sunacaktır.

Yetkili Denetim Kurumunun BCR-P’ye uyumun denetimini yapmasıyla ilgili herhangi bir anlaşmazlık söz konusu Denetim Kurumunun Üye Devletinin mahkemeleri tarafından, bu Üye Devletin usul hukukuna uygun olarak çözülecektir. BCR Üyeleri kendilerini bu mahkemelerin yargı yetkisine tabi tutmayı kabul ederler.

1. BCR’yi kapsayan denetim programı

Veri İşleyen olarak hareket eden her BCR Üyesi, BCR-P’ye uyumdan sorumlu olacak ve bu uyumu gösterebilecektir. Bu amaçla ve Madde 4.4 (İşleme Faaliyetlerinin Kaydı) ve Madde 4.5’te (Güvenlik) belirtilen gerekliliklere ek olarak, BCR Üyeleri veri koruma denetim programıyla ilgili aşağıdaki gerekliliğe uyacaktır.

BCR Üyesi, denetim programını geliştirmeyi ve işbu BCR-P’ye uyumunun incelenmesini denetim programına entegre etmeyi taahhüt eder. Denetim programı, şunları tanımlamayı sağlayacaktır:

* Denetimlerin gerçekleştirileceği makul bir sıklık,
* Denetimin beklenen kapsamı ve
* Denetimden sorumlu ekip.

Denetim prosedürü, **Ek 7 – Veri Gizliliği Denetimleri Prosedürleri**’nde ayrıntılı olarak açıklanmıştır. Denetim, düzeltici aksiyonların alınmasını sağlayacak yöntemler ve aksiyon planları dahil olmak üzere işbu BCR-P’nin tüm yönlerini (örneğin; uygulamalar, BT sistemleri, kişisel verileri işleyen veri tabanları veya ileriye dönük aktarımlar, BCR-P ile çelişen ulusal yasalar kapsamındaki zorunlu gerekliliklerle ilgili alınan kararlar, Gruptan Veri İşleyenlere yapılan aktarımlar için kullanılan sözleşme şartlarının incelenmesi, düzeltici aksiyonlar, vs.) kapsar. Bununla birlikte bir BCR Üyesi için BCR-P’nin tüm yönleri uygun düzenli aralıklarla izlendiği sürece, söz konusu BCR Üyesi her denetlendiğinde bu tür bir denetim programının BCR-P’nin tüm yönlerini izlemesi gerekmez.

BCR Üyeleri, BCR-P’ye uyumun doğrulanmasını veya işbu BCR-P kapsamına giren bir Veri İşleme faaliyetinin İlgili Kişilerin hak ve özgürlükleri üzerindeki risk seviyesinin dikkate alınmasını sağlamak için düzenli olarak (en azından yılda bir kez ve/veya uyumsuzluk belirtileri varsa) denetimler yapılmasını taahhüt eder.

Düzenli denetimlere ek olarak, DPO ve/veya ilgili gizlilik ağı üyesi (ör. Yerel Gizlilik Lideri) ya da Concentrix Grubu’ndaki iç denetim departmanı gibi diğer bir yetkili fonksiyon tarafından özel denetimler (ad hoc denetimler) talep edilebilir. Söz konusu denetimler, DPO ve/veya ilgili gizlilik ağı üyesi tarafından tavsiye edilen dahili ve/veya harici akredite denetçiler tarafından gerçekleştirilebilir. Yol haritası, Ek 7’de belirtildiği gibi DPO ve/veya ilgili gizlilik ağı üyesi tarafından başlatılır ve belirlenir. Her halükarda harici denetçiler bağımsız, bir gizlilik yükümlülüğüne tabi ve/veya uygun bir yasal gizlilik yükümlülüğü altında olacaktır.

DPO, gerçekleştirilecek denetimlerin kapsamını belirlemekten sorumludur. Bu amaçla Gizlilik Komitesine danışabilir ve/veya söz konusu denetimin kapsamını belirlemek üzere Concentrix’in iç denetim ekibine güvenebilir. Denetim, aşağıdaki koşullar sağlandığı takdirde Grup DPO’su ve/veya ilgili gizlilik ağı üyeleri (ör. Yerel Gizlilik Lideri) ve/veya Concentrix Grubu’nun iç denetim ekibi veya Concentrix bünyesindeki başka bir ilgili fonksiyon tarafından yapılabilir:

* Sorumlu kişilere, bu denetimlere ilişkin görevlerinin yerine getirilmesi konusunda bağımsızlık güvencesi verilmesi ve
* BCR-P’ye uyumu denetlemekten sorumlu kişiler için söz konusu durumun bir çıkar çatışmasına yol açması.

Her denetimin sonucu, bilgi amaçlı Grup DPO’suna ve/veya ilgili gizlilik ağı üyelerine (ör. Yerel Gizlilik Liderleri) ve/veya Gizlilik Komitesi ve/veya Webhelp SAS yönetim kurulu üyelerine sunulacaktır. Nihai rapor, kusur tespiti ve düzeltici aksiyonlar Yerel Gizlilik Lideri tarafından paylaşılacak ve uygulanacaktır. Yerel Gizlilik Lideri değerlendirmesine dayanarak rapor, uygun olduğu hallerde herhangi bir İş Gizlilik Uzmanı, yerel güvenlik yöneticisi, süreç/sistem sorumluları, Concenrix Grubu nihai ana şirketinin yönetim kurulu veya denetime tabi ilgili BCR Üyesinin yönetim kurulu veya herhangi bir diğer gerekli kurum içi çalışanla da paylaşılabilir. Öncelikli olarak söz konusu önlemlerin uygulanmasıyla birlikte düzeltici aksiyonlar tanımlanacaktır.

Concentrix, yetkili AEA Denetim Kurumlarının ve BCR Üyelerinin Müşterilerinin, denetimden doğrudan etkilenmeleri halinde, denetim sonuçlarının iletilmesini talep edebileceklerini ve dolayısıyla talep edilmesi halinden bunlara erişim imkanı tanımayı kabul ettiklerini onaylar. Denetim raporlarının ve ilgili iç denetim raporlarının sonuçları, AEA’da bulunan Denetim Kurumlarının aşağıda belirtilen denetim haklarını kullanmaları halinde bunlara erişebilecekleri bir biçimde tutulacaktır. Ayrıca Veri İşleyen veya Alt Veri İşleyen olarak hareket eden BCR Üyeleri, Veri Sorumlusunun talebi üzerine Veri Sorumlusu ile ilgili Veri İşleme faaliyetlerinin denetimi için İşleme olanaklarını sunmayı taahhüt eder.

BCR Üyeleri, Yetkili Denetim Kurumlarının talep etmeleri halinde denetim sonuçlarına erişebilmesini sağlamayı taahhüt eder ve özellikle ticari sırların korunması gibi bir gizlilik gerekçesiyle bu hakları sınırlamaz.

BCR Üyesinin herhangi bir yetkili AEA Denetim Kurumuna BCR-P ile ilgili herhangi bir konuda veri koruma denetimleri yapma yetkisi vereceği hatırlatılır. Bu bağlamda her BCR Üyesi, AEA Denetim Kurumunun BCR Üyelerinin işbu BCR-P’ye uyumunu göstermek için gerekli bilgileri elde edebilmesi için ilgili BCR Üyesini denetlemesine izin verecektir (ayrıca bkz. yukarıda Madde 13.4).

Ayrıca bir BCR Üyesinin Veri İşleyen olarak hareket ettiği durumlarda Müşterileri, makul aralıklarla ve her durumda yılda bir kereden fazla olmamak üzere, makul bir süre önceden bildirimde bulunarak ve masrafları kendisine ait olmak üzere Concentrix’in kendisinin veya alt veri işleyenlerin Hizmet Sözleşmesi ve/veya Veri İşleme Sözleşmesi ile işbu BCR-P’ye uyumunu değerlendirmek için denetimler yapmasını talep edebilir.

Bu durumda BCR Üyesi; Geçerli Veri Koruma Mevzuatı, işbu BCR-P ve geçerli Veri İşleme Sözleşmesine riayet edildiğini göstermek için Müşteriye gerekli tüm bilgileri sunacak ve Müşteri veya Hizmet Sözleşmesi uyarınca Müşteri tarafından yetkilendirilen başka bir denetçi tarafından yürütülen denetimlere (teftişler dahil) izin verecek ve katkıda bulunacaktır.

Bu Denetim, Ek 07’de belirtilen prosedüre uygun olacaktır.

1. BCR-P’de değişiklik

Concentrix DPO, Yerel Gizlilik Liderlerinin desteğiyle işbu BCR-P’nin güncel tutulmasını sağlayacaktır (örneğin; düzenleyici ortamda yapılan değişiklikleri, AB veri koruma kurumlarının nerilerini veya BCR-P kapsamındaki değişiklikleri hesaba katmak için).

Özellikle DPO, BCR-P’ye tabi olan kuruluşların listesini güncel tutacaktır. Concentrix’in herhangi bir yeni kuruluşu BCR-P’ye etkin bir şekilde tabi olduğunda (Madde 3.2’de belirtildiği üzere) DPO bu listeyi güncelleyecek ve fazla gecikmeden tüm BCR Üyelerini ve ilgili AEA Denetim Kurumlarını yetkili AEA Denetim Kurumu vasıtasıyla bilgilendirecektir. Bu tür güncellenmiş bilgiler, İlgili Kişilere BCR-P ile birlikte ve aynı yollarla sunulacaktır.

Webhelp SAS, bu tür değişiklikleri yılda en az bir kez veya DPO tarafından gerekli görüldüğünde yetkili AEA Denetim Kurumlarına bildirecektir. Söz konusu değişiklikler, AEA Denetim Kurumlarına yılda en az bir kez güncellemeyi gerekçelendiren nedenlerin kısa bir açıklamasıyla birlikte yetkili AEA Denetim Kurumu vasıtasıyla bildirilecektir. Hiçbir değişiklik yapılmadığında da Denetim Kurumlarına aynı süreci takiben yılda bir kez bildirim yapılmalıdır.

Yıllık güncelleme veya bildirim, Sorumlu BCR Üyesi olarak Webhelp SAS’ın, BCR-P’nin AEA dışındaki BCR Üyeleri tarafından ihlalinden kaynaklı zararların tazminini sağlamak için uygun düzenlemeler yaptığına ilişkin teyidin yenilenmesini de içermelidir.

Bir değişikliğin BCR-P üzerinde veya işbu BCR-P tarafından verilen hakların korunma seviyesi üzerinde önemli bir etkisi olduğu ölçüde Webhelp SAS, DPO’nun yardımıyla BCR Üyelerini ve AEA Denetim Kurumlarını derhal bilgilendirmeyi taahhüt eder.

1. BCR-P’ye uyulmaması

Veri Sağlayıcısı ve Veri Alıcısı, bir BCR Üyesi olarak aşağıdaki gerekliliklere uyacaktır:

* Bir BCR üyesi BCR-P’ye etkin bir şekilde tabi olmadığı ve buna uyumu sağlayamadığı sürece bu BCR üyesine hiçbir veri aktarımı yapılmaz.
* Veri Alıcısı, yukarıda BCR-P Madde 13.3’de daha ayrıntılı olarak açıklanan durumlar dahil olmak üzere herhangi bir nedenle BCR-P’ye uyamadığı takdirde Veri Sağlayıcısını derhal bilgilendirmelidir.
* Veri Alıcısı, BCR-P’yi ihlal eder veya BCR-P’ye uyamazsa Veri Sağlayıcısı veya Müşteri Veri Aktarımını askıya almalıdır.

Veri Alıcısı, aşağıdaki durumlarda Veri Sağlayıcısının tercihi üzerine BCR-P kapsamında Aktarılmış olan Kişisel Verileri derhal iade edecek veya silecektir:

* Veri Sağlayıcısı veri aktarımını askıya almışsa ve işbu BCR-P’ye uyum makul bir süre içinde ve her halükarda askıya alınmadan itibaren bir ay içinde düzeltilmezse,
* Veri Alıcısı, BCR-P’yi önemli veya sürekli olarak ihlal ediyorsa,
* Veri Alıcısı, BCR-P kapsamındaki yükümlülüklerine ilişkin yetkili bir mahkemenin veya Yetkili Denetim Kurumunun bağlayıcı bir kararına uymuyorsa.

Aynı taahhütler, verilerin tüm kopyaları için geçerli olmalıdır. Veri Alıcısı, verilerin silindiğini Veri Sağlayıcısına onaylamalıdır.

Veriler silinene veya iade edilene kadar Veri Alıcısı, BCR-P’ye uyumu sağlamaya devam etmelidir.

Veri Alıcısı için geçerli yerel yasaların aktarılmış olan Kişisel Verilerin iadesini veya silinmesini yasaklaması durumunda Veri Alıcısı, BCR-P’ye uyumu sağlamaya devam edeceğini ve verileri yalnızca bu yerel yasa uyarınca gerekli olduğu ölçüde ve süre boyunca işleyeceğini garanti etmelidir.

Yürürlükteki yerel yasaların ve/veya uygulamaların BCR-P’ye uyumu etkilediği durumlar için, bkz. yukarıda BCR-P Madde 13.3.

1. Fesih

Veri Alıcısı olarak hareket eden ve BCR-P’ye tabi olmaktan çıkan bir BCR Üyesi, BCR-P kapsamında alınan Kişisel Verileri saklayabilir, iade edebilir veya silebilir.

Veri Sağlayıcısı ve Veri Alıcısı, verilerin Veri Alıcısı tarafından saklanabileceği hususunda anlaşırsa GDPR Bölüm V doğrultusunda ve BCR-P Madde 6’da yansıtıldığı şekilde koruma sürdürülmelidir.

1. Ekler

* Ek 01 - BCR-P’ye tabi Concentrix kuruluşları ve yerel gizlilik e-posta iletişim listesi
* Ek 02 - Bağlayıcı Şirket Kuralları (BCR) ve Prosedür Tanımları
* Ek 03 - Gizlilik Yönetimi ve organizasyonu
* Ek 04 - Gizlilik farkındalığı ve eğitim programı
* Ek 05 BCR Üyelerinin Veri Sorumlusu olarak hareket ettiği durumlarda İlgili Kişilerin taleplerine ilişkin prosedür
* Ek 06 - BCR Üyelerinin Veri İşleyen olarak hareket ettiği durumlarda İlgili Kişilerin taleplerine ilişkin prosedür
* Ek 07 - Denetim Prosedürü
* Ek 08 - Kişisel Verilerin İhlali Prosedürü
* Appendix 09 - Veri Koruma Etki Değerlendirmesi
* Ek 10 - Bilgi Güvenlik Politikası
* Ek 11-A Veri İşleme Amaçları ve ilgili Kişisel Veri ve İlgili Kişi Kategorileri BCR-C Listesi (Maddi Kapsam)
* Appendix 11-B Veri İşleme Amaçları ve ilgili Kişisel Veri ve İlgili Kişi Kategorileri BCR-P Listesi (Maddi Kapsam)

BELGE KONTROLÜ

|  |  |  |
| --- | --- | --- |
| Versiyon | Güncelleme | Değişiklik Özeti |
| 0.1 | 27/02/2022 | Son Onay |
| 0.2 | 01/01/2023 | BCR Üyeleri listesinin güncellenmesi |
| 0.3 | 24/02/2023 | BCR Üyeleri listesinin güncellenmesi |
| 0.4 | 01/04/2024 | Yeniden markalama ve biçimlendirme  Yeni EDPB tavsiyesinin ilgili hükümleriyle kısmi uyum BCR Veri Sorumlusu hakkındaki Tavsiyeler 1/2022 (WP56\_Rev01’i yürürlükten kaldıran ve değiştiren) |

|  |  |
| --- | --- |
| İnceleme Sıklığı | Bu belge en az yılda bir kez veya Webhelp kuruluşlarında değişiklik olduğunda gözden geçirilecektir. |
| Düzenleme Tarihi | 25/05/2018 |
| Alan | Gizlilik |
| Sınıflandırma | Kamuya Açık |
| Referans | EN\_\_GPPriv-01- Bağlayıcı Şirket Kuralları - Veri İşleyen |